UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

ARQUITECTURAS Y SEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL E IoT PARA INFRAESTRUCTURAS CRÍTICAS

Trabajo Fin de Máster

Máster Universitario en Ciberseguridad y Ciberinteligencia

AUTOR/A: Saiz Miranda, Javier

Tutor/a: Palau Salvador, Carlos Enrique

CURSO ACADÉMICO: 2021/2022

Dedicatoria

A mis hijos que marcan mi Norte.

Ellos me animan a seguir formándome en lo académico y en todo lo demás.

El objetivo: estar a su altura y hacer por no fallarles.

Por ellos.

Agradecimientos

Agradezco el apoyo recibido de la institución que me ha financiado y que ha dado forma a mi vida los últimos 20 años., haciéndome en cierta manera lo que soy y de lo que estoy orgulloso.

Gracias

Resumen

El auge del uso y la evolución tecnológica de IoT en entornos industriales (IIoT) y más en particular en infraestructuras críticas para el funcionamiento de nuestra sociedad está haciendo necesario una revisión de las arquitecturas para esas infraestructuras. La arquitectura debe tener en cuenta las nuevas necesidades y las nuevas capacidades. La superficie de ataque en sistemas de control industrial (SCI / SCADA), también denominados OT, que además incorporan IoT, se incrementa sensiblemente por la variedad de tecnologías, fabricantes y sobre todo de capacidades entre los distintos elementos que lo conforman. A mayor superficie de ataque más complicado es identificar una arquitectura SCI segura. Determinar una arquitectura donde configurar elementos, protocolos, comunicaciones, criptografía, sistemas IT, sistemas de supervisión y monitorización, etc. donde implementar unos sistemas de ciberseguridad conforme a unas políticas y recursos resulta el reto al que se enfrenta este TFM. Asimismo el objetivo adicional es el implementar un elemento de ciberseguridad como puede ser un IDS en un entorno reproducible con los medios al alcance.

Palabras clave: arquitectura, IoT, IIoT, Sistemas de Control Industrial SCI, SCADA.

Resum

L'auge de l'ús i l'evolució tecnològica d'IoT en entorns industrials (IIoT) i més en particular en infraestructures crítiques per al funcionament de la nostra societat fa necessari una revisió de les arquitectures per a aquestes infraestructures. L'arquitectura ha de tenir en compte les necessitats noves i les noves capacitats. La superfície d'atac en sistemes de control industrial (SCI/SCADA), també anomenats OT, que a més incorporen IoT, s'incrementa sensiblement per la varietat de tecnologies, fabricants i sobretot de capacitats entre els diferents elements que el conformen. A més superfície d'atac més complicat és identificar una arquitectura SCI segura. Determinar una arquitectura on configurar elements, protocols, comunicacions, criptografia, sistemes IT, sistemes de supervisió i monitorització, etc. on implementar uns sistemes de ciberseguretat d'acord amb unes polítiques i recursos resulta el repte a què s'enfronta aquest TFM. Així mateix l'objectiu addicional és implementar un element de ciberseguret

Paraules clau: arquitectura, IoT, IIoT, Sistemes de Control Industrial SCI, SCADA.

Abstract

The boom in the use and technological evolution of IoT in industrial environments (IIoT) and more particularly in critical infrastructures for the functioning of our society is making it necessary to review the architectures for these infrastructures. The architecture must take into account new needs and new capabilities. The attack surface in industrial control systems (ICS / SCADA), also called OT, which also incorporate IoT, increases significantly due to the variety of technologies, manufacturers and, above all, the capabilities of the different elements that comprise it. The larger the attack surface, the more difficult it is to identify a secure SCI architecture. Determine an architecture where to configure elements, protocols, communications, cryptography, IT systems, supervision and monitoring systems, etc. where implementing cybersecurity systems in accordance with policies and resources is the challenge that this TFM faces. Likewise, the additional objective is to implement a cybersecurity element such as an IDS in a reproducible environment with the means available.

Keywords: architecture, IoT, IIoT, Industrial Control Systems ICS, SCADA.

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Es evidente en cada artículo que leemos o cada vez que entramos en contacto con los medios de comunicación la mayor relevancia que tienen las infraestructuras críticas para una sociedad normal en un país medianamente desarrollado, que quiera mejorar su desarrollo, o simplemente conservarlo.

Las infraestructuras críticas, en la mayoría de los casos, son controladas, supervisadas y gestionadas por Sistemas de Control Industrial, o lo que viene a llamarse de una manera más general OT (*Operational Technologies*).

Paralelamente se van desarrollando dos conceptos: las tecnologías de la información (IT en terminología inglesa) y el Internet de las cosas (IoT, que aplicado a entornos industriales sería IIoT), que van desarrollando potencia, capacidad, dependencia de los usuarios a su utilización, etc. El uso y el magnifico desarrollo de las IT se basa en su imbricación en todas y cada una de las actividades diaria de cualquier individuo de cualquier sociedad (o casi). Para el caso de IIoT es el abaratamiento de costes, la facilidad de diseño y el incremento de capacidades a bajo coste son las razones de su rápido crecimiento (sin dejar de lado la, cada día mayor, presencia de dispositivos IoT en nuestros quehaceres).

La convergencia de los tres mundos, con un denominador común que es la tecnología, pero con unas características de base y de "mercado objetivo" tan distintas es ya un hecho. Es imposible pensar en una infraestructura crítica que no solo incorpore los sistemas de control industrial tradicionales, sino las capacidades de IoT/IIoT para el control de parámetros de campo, y además IT para la gestión en todos los niveles más allá de lo puramente operacional (de gestión, de negocio, de proceso, de control, de administración, de supervisión etc.).

La suma de las capacidades de los tres mundos no es algorítmica, pues tanto sus ventajas como sus inconvenientes se disparan al considerarlo como un todo. Únicamente pensando en la ciberseguridad, que es el objetivo del Master y de este TFM, las posibilidades se incrementan de manera exponencial. La superficie de ataque de un sistema no se suma a la de otro, se añade y se configura como un todo que requiere un paso atrás y un replanteamiento de la arquitectura de un sistema "nuevo" a proteger.

El objetivo principal del TFM es hacer un estudio de las arquitecturas existentes con esas tecnologías convergentes y proponer una estructura de arquitectura genérica que integre la configuración de elementos, protocolos, comunicaciones, criptografía, sistemas, sistemas de supervisión y monitorización, etc. conforme a unas políticas y recursos con la seguridad como un requisito de diseño, de desarrollo y en general para todo el ciclo de vida de los sistemas que se ajusten a ella.

El reto esta en la generalización de conceptos muy heterogéneos que actualmente no siempre se integran pensando en la seguridad, sino en la operatividad, la rentabilidad, valores de negocio, etc. De ahí la necesidad de la implantación de estas arquitecturas, en constante desarrollo aunque un paso por detrás de la evolución de los elementos individuales, que en el caso de IoT/IIoT seria de varios pasos atrás por como son de dinámicos, frente a sistemas mas complejos e integrados en un todo.

2. Motivación

La seguridad en redes de información y telecomunicaciones es algo que ya no hace falta ni plantear como una necesidad. Se entiende como tal. Si esta necesidad es asumida para un negocio, mucho mas es para un servicio público. Cuando ese servicio público es ofrecido por una infraestructura crítica para el funcionamiento de la sociedad, parece un requisito irrenunciable para los que desarrollamos nuestro día en aras de una sociedad mejor y más segura.

Una arquitectura basada en la seguridad por diseño, con todos sus elementos nacidos con esos mismos principios e integrados en un sistema que ofrezca máxima resistencia a elementos externos que persiguen su deterioro es el objetivo que toda organización desearía tener.

Hablar de seguridad de una organización es una cosa y cuando se habla del país en el que uno vive todo cobra mucho más entidad. Lo que mueve a dar seguridad es la protección de una sociedad en la que vivimos.

A riesgo de haber sido demasiado extenso el razonamiento, son necesarios los tres párrafos anteriores para plantear la principal motivación. Además del deseo de proteger y servir a la sociedad del país en el que vivimos a través de unas infraestructuras críticas que funcionen con las máximas garantías, existen otras motivaciones que aun siendo menos importantes, se relacionan con la anterior y son necesarias: las tecnológicas, las económicas, etc.

La definición de una arquitectura uniforme para sistemas de control industrial integrados en infraestructuras críticas es el objetivo de este trabajo y debe ser garantizar:

- la conservación de aquellos sistemas que no han podido evolucionar pero que siguen dando servicio (*legacy*).
- la evolución de sistemas flexibles existentes hacia un conjunto mas robusto
- la incorporación de nuevas tecnologías que puedan marcar una superficie de exposición de esas infraestructuras con el menor numero de vulnerabilidades posibles independientemente de si son elementos más o menos inteligentes o capaces, o de uno o varios proveedores, o con una procedencia u otra.

Y de esta manera, el presente TFM aunando los valores originales de la primera arquitectura, los nuevos conceptos definidos en sistemas de control industrial, IoT e IIoT (Cyber Security 4.0: Protecting the Industrial Internet of Things, s.f.), las nuevas normas nacionales e igualmente las internacionales se define una arquitectura integradora, simplificada y ajustada a requerimientos nacionales para poder contar con los medios de seguridad que una entidad acreditada la valide y le otorgue un sello de garantía que sin duda de valor al sistema..

3. Objetivos

Los objetivos básicos de este trabajo son:

Objetivo 1	Establecer una arquitectura segura para sistemas de control industrial que integren IoT.
Descripción	Desarrollar, respaldar y plantear un caso de uso que valide una solución holística y disruptiva que permita la seguridad para la prevención y protección contra ataques dirigidos a sistemas de control industrial que incorporen IoT. Todo esto sin mermar las capacidades de mejora de los sistemas y menoscabar la efectividad y eficiencia existentes.
Resultados esperados	Generar una arquitectura lo bastante genérica para que todo tenga cabida, pero con los elementos necesarios para que de forma concreta se adquiera seguridad.
Verificación	Integración por niveles y zonas de seguridad entre ellos (DMZs)

Objetivo 2	Definir unas condiciones de contexto tecnológicas, normativas, políticas, etc. que integren al máximo las exigencias necesarias para lo que se considera seguridad.
Descripción	Mostrar un estado del arte de los sistemas de control industrial y sus arquitecturas tanto reales como propuestas por aquellas entidades reguladoras de ámbito internacional y nacional para ofrecer un paradigma unificado que afronte los retos tecnológicos (inteligencia artificial, *blockchain, edge computing*, etc.) como una oportunidad de mejorar en la seguridad ante ataques.
Resultados esperados	Definir elementos y áreas de trabajo (de una fabrica, de una oficina, de una red, etc.) que deben dibujarse y trasladarse en una organización
Verificación	Agrupación por elementos, niveles y áreas de trabajo de todos aquellos elementos (físicos o no)

Objetivo 3	Establecer los elementos necesarios en la tecnología, en los procesos, en las políticas, etc. para una arquitectura segura.
Descripción	Aprovechar los entornos, la documentación y las conclusiones de los grupos de trabajo y organizaciones mas innovadoras donde los pilares son la seguridad, la privacidad, la responsabilidad, la confiabilidad, etc., así como ofrecer anticipación, detección, seguimiento, mitigación e información al usuario final de comportamientos maliciosos y anómalos casi en tiempo real, dentro de las aplicaciones y procesos de los sistemas de control industrial.

Resultados esperados	Definir de manera práctica, bajando de nivel respecto al objetivo 2, aquello necesario para obtener seguridad.
Verificación	Recomendación de sistemas y herramientas.

Objetivo 4	Plantear un caso de uso
Descripción	Sobre una infraestructura crítica, elegir un sistema de control industrial y definir una arquitectura de aplicación tan real como teórica. No obstante se darán herramientas reales para la implementación, en su mayor parte opensource y sobradamente reconocidas por los profesionales del sector.
Resultados esperados	Una arquitectura real con seguridad conforme a norma y recomendación
Verificación	Niveles, zonas de seguridad y elementos.

.

Cuatro tres objetivos fundamentales que se podrían plasmar en un caso de uso que demuestre los anteriores:

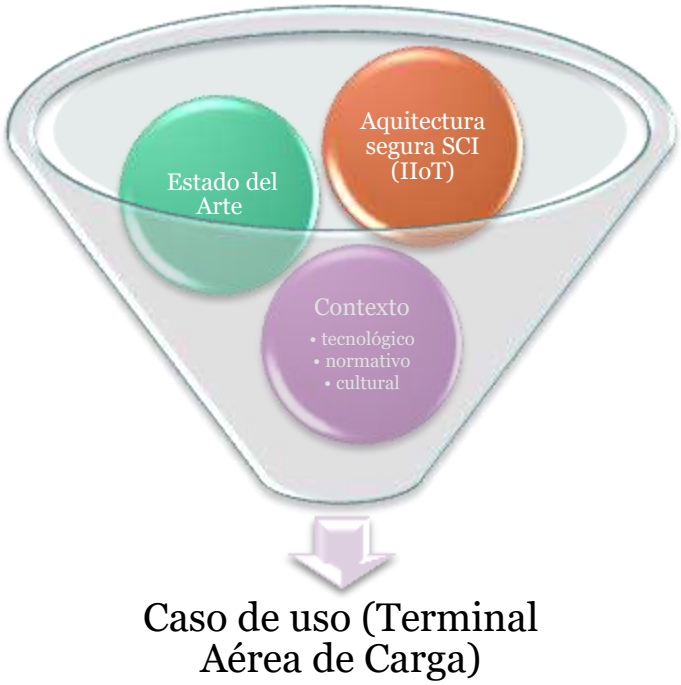


Figura 1 .- Objetivos fundamentales del TFM

4. Impacto Esperado

El presente TFM tiene el reto de generar un impacto sobre varios frentes pero sobre el mismo elemento: ***la seguridad***. Los frentes sobre los que se pretende aportar son:

- La concienciación del uso de arquitecturas seguras en todo sistema de control industrial, por más tiempo que este tenga. Se espera que todo aquel que lea estas líneas tenga el convencimiento de que la seguridad se puede mejorar siempre pues aunque la seguridad total no existe, lo que esto da es margen de mejora en el que trabajar. Todo cambio debe partir de un convencimiento de que es a mejor y solo a partir de trabajos teóricos y/o prácticos se va "educando" a empleadores y empleados de empresas y entidades relacionadas con los sisemas que nos ocupan.
- La definición de una arquitectura global de la que cualquier proveedor de servicios pueda extraer un modelo que se adapte a su infraestructura, por pequeña o grande que sea, y le aporte seguridad y garantías. Se espera que todas los sistemas de control industrial e infraestructuras críticas vean la seguridad como algo alcanzable ajustándose a un modelo versátil y eficaz
- La propuesta de herramientas opensource para la implementación de la arquitectura o la simulación de entornos. Todo aquel colectivo relacionado con los sistemas aquí mencionados verán la posibilidad de implementar escenarios de simulación y prueba para ejecutar una implemetación posterior caso de ser necesario al menor conste posible y con un impacto en seguridad elevado pero el menor posible en la eficiencia del entorno industrial.

Si se logra impactar en esos tres frentes y fomentar la aceptación de la recomendación de la arquitectura supondría asegurar la adaptación de un sistema de control industrial a un marco normativo que marca requisitos mínimos de seguridad conforme a los cuales se acreditan los elementos de sistemas mayores y da lugar a un proceso integrador a nivel nacional e internacional.

El efecto en la comunidad educativa puede ser simplemente de aumento de la literatura, y de los estudios de integración de normativa, aunque en el ámbito de la seguridad de infraestructuras críticas sería una nueva relación de arquitecturas pasadas, presentes y lo que podría ser una futura. Esa comunidad educativa puede desarrollar las arquitecturas planteadas con las herramientas que se ofrecen para favorecer el aprendizaje y la investigación (o al menos colaborar humildemente en este sentido) en la seguridad en escenarios simulados, trasladados e incluso reales por tratarse de software libre pero de amplia difusión y uso.

Además de lo anterior, y en base en la ficha final de este TFM, se demuestra la posibilidad de alcanzar mediante esa arquitectura convivencia y conveniencia para con los valores promovidos por las Naciones Unidas (United Nations, s.f.) y relacionados con quince objetivos globales *"para erradicar la pobreza, proteger el planeta y asegurar la prosperidad de todos como una parte de una nueva agenda de desarrollo sostenible"*. La arquitectura que se espera conseguir impacta de manera muy directa en un alto porcentaje de esos quince objetivos. Para y tal y como se ve en los Objetivos de Desarrollo Sostenible el impacto de la seguridad y establecimiento de una arquitectura común

básica para todo sistema de control industrial integrado en una infraestructura crítica puede conducir a un mundo mejor en múltiples aspectos. La seguridad como base del equilibrio entre los componentes de una sociedad que comparte un planeta llamado Tierra. Esa seguridad siempre bien entendida y orquestada entre los distintos actores para lograr un equilibrio entre los intereses de todos sin menoscabo del bienestar de nadie y mucho menos atentando a los derechos universales de todo ser humano y consideraciones propias al ecosistema global del planeta.

5. Estructura

La estructura general de desarrollo del trabajo y eliminando la parte menos técnica, es la comentada más arriba y que viene a ser la siguiente:

- PARTE I Estado del arte donde se describen:
    - Los elementos de un sistema de control industrial de cualquier infraestructura crítica
    - Los niveles básicos en los que colocar dichos elementos dentro de un sistema y de una organización (empresa, industria, etc.)
    - Como gestionar los elementos y su seguridad
- PARTE II Análisis del problema, donde se describen:
    - La normativa aplicable en el ámbito internacional
    - Las guías y recomendaciones de las autoridades nacionales
    - La descripción de una infraestructura crítica y un sistema de control industrial donde aplicar una arquitectura.
    - La necesidad surgida y la solución planteada: una arquitectura de un sistema de control industrial en el caso de uso.
- PARTE III Solución propuesta al problema, donde se describen:
    - Los elementos a utilizar
    - Los niveles de arquitectura a implementar
    - Las herramientas disponibles (opensource, trial, etc.)
    - Una implementación inicial.

6. Estado del arte

6.1. ARQUITECTURAS Y DISPOSITIVOS DE CAMPO

6.1.1. Superficie de ataque en un SCI. Generalidades

Para identificar la superficie de ataque 1de un sistema de control industrial (en adelante SCI o ICS *Industrial Control System*) se pueden utilizar los criterios de distintas normas y recomendaciones:

- NIST CSF V1.1
- ISA/IEC 62443-2-1:2009
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev.4
- CIS CSC
- COBIT 5

Todos los textos anteriores se basan en la intención que puede tener un actor externo a un sistema objetivo basado o que incluye "tecnología operacional" (Operational Technologies OT) o sistemas de control industrial (SCI).

Las intenciones del atacante pueden ser de lo mas variopintas ya que los SCI están imbricados en la mayoría de las infraestructuras críticas de cualquier nación y juegan un papel fundamental en la generación de riqueza y poder de dicha nación o simplemente en el funcionamiento habitual de cualquier sociedad. Por lo tanto los motivos que se pueden tener para llevar a cabo un ataque son muchos:

- arruinar o encumbrar a un país o región
- espionaje industrial
- terrorismo
- espionaje gubernamental o ciberdefensa nacional
- hacktivismo
- entrenamiento basado poner a prueba a un sistema o un equipo de forma controlada

La forma en la que un ataque se lleva o podría llevarse a efecto va a determinar la forma de defenderse de él. Para identificar dicha formula de ataque, y que va a dar una imagen de lo vulnerable que es el sistema, se valoran dos factores fundamentalmente:

[1] Ejemplos de ciber ataques a SCI son:

- Hack attack causes 'massive damage' at steel works - BBC News
- Ransomware Attack Disrupts San Francisco Rail System | SecurityWeek.Com
- Attackers Alter Water Treatment Systems in Utility Hack: Report | SecurityWeek.Com
- Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure | *Mandiant*

- modelos de ataque aplicables a un sistema, que indicarían como un atacante podría atacar un sistema mediante diagramas o esquemas
- superficie de ataque de un sistema, que indicaría los puntos que un atacante podría usar para atacar

Cuanto menor sea la superficie de ataque, más resistente a los ataques será el sistema. Así el analizar la superficie de ataque o los modelos aplicables a un sistema determinado da una idea de la debilidad de ese sistema y de cómo mejorar su resiliencia.

Para identificar la superficie de ataque de un determinado sistema o elementos de un SCI lo mejor es ir de alto a bajo nivel:

- Alto nivel sería contemplar los ataques procedentes de fuera del SCI (sistemas de cualquier parte de la organización a la que pertenece el SCI como otras redes, DMZs, etc. haciendo uso de ataques *client-side* o *insiders* entre otros), e incluso de fuera de la organización (internet, y una vez en la capa de negocio es solo cuestión de tiempo el acceder a otros niveles mas bajos como son las redes de control o de dispositivos y que veremos mas abajo).
- Pensar en ataques a bajo nivel es pensar en unos escenarios distintos y mas concretos como son los accesos remotos a las redes de control y de ahí a las redes de campo o mediante, por ejemplo, malware introducido con USB' s o similar directamente en terminales de estas redes.

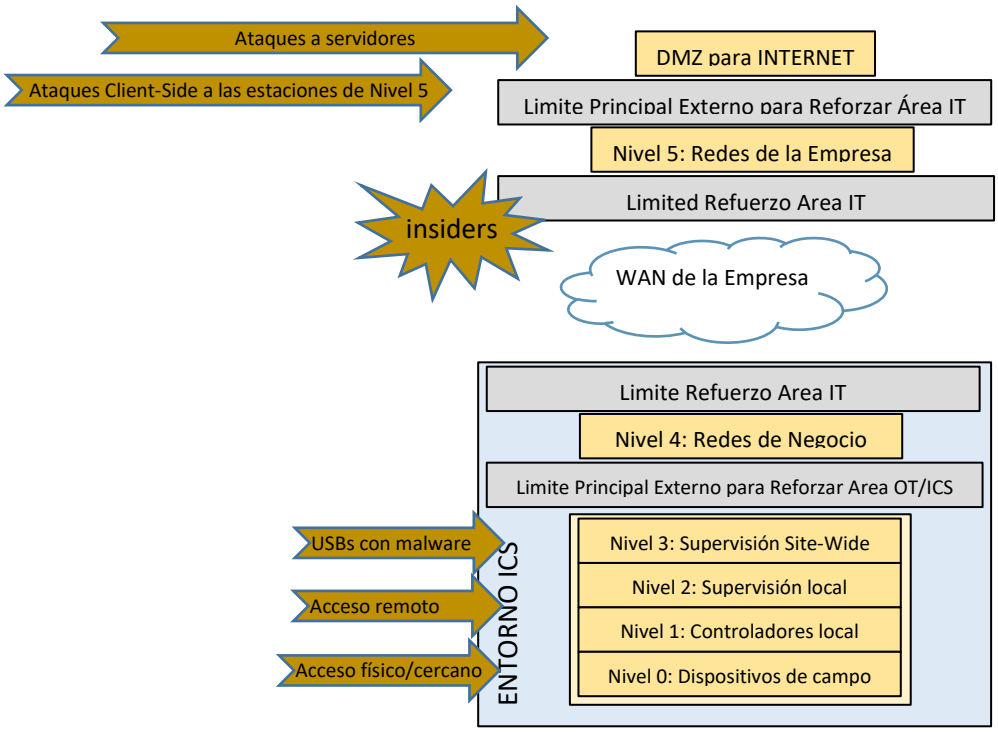


Figura 2 .- Superficie de ataque

En ese bajo nivel, si se considera la red de control (red de control de dispositivos de control programables, dispositivos finales de un SCI, etc.) en particular se debe tener en cuenta que una vez el atacante ha accedido a ella puede comprometer cualquier dispositivo de dicha red que tendrán distintas tecnologías, fabricante, etc. y por lo tanto superficies de ataques propias. Así por ejemplo:

- las estaciones (servidores) de gestión suelen ser maquinas comunes con sistemas operativos ampliamente utilizados (Windows, Linux, etc.) y que si no están actualizados (y pueden no estarlo por no estar conectados a Internet) tienen multitud de vulnerabilidades mas que conocidas por el atacante. La explotación de dichas vulnerabilidades (una vez el intruso hace llegar el SW adecuado a tal efecto por la vía que sea, como p. ej. acceso físico no autorizado) puede dar lugar a que lo que no esté conectado, permita movimientos laterales que den lugar a conexión propia o de terceros dispositivos.
- esas estaciones u otras y HMI tiene interfaces y aplicaciones basadas en web que pueden tener fallos también muy conocidos en el mundo de la seguridad ciber y que se pueden utilizar para pasar los controles de autenticación y suplantar una identidad y actuar como tal, instalar SW, etc.
- las redes de comunicación entre maquinas de supervisión en su mayoría se basan en TCP/IP y no disponen de medidas de seguridad o son fáciles de superar por el atacante. Para otros niveles hay multitud de protocolos, algunos de ellos propietarios donde, en muchos casos, la seguridad no estaba entre sus requisitos de diseño. Resulta fácil llevar a efecto determinado ataques como son los de denegación de servicio y especialmente esa denegación pero con carácter distribuidos si se aprovecha la infraestructura compuesta por muchos dispositivos sencillos, no seguros que sirvan para atacar un punto desde donde se da un servicio común a la red (DoS y DDoS)
- los dispositivos pueden estar accesibles físicamente para el atacante y éste puede manipularlos para actuar directamente sobre un proceso o acción o bien actuar sobre la electrónica existente en el dispositivo para modificar el comportamiento normal del sistema, en ese dispositivo o en otro de dicho ecosistema. Esta posibilidad de actuación sobre los elementos finales de manera directa abre la opción de ataques a otros dispositivos del mismo nivel o subir a servidores y contenidos de orden superior.

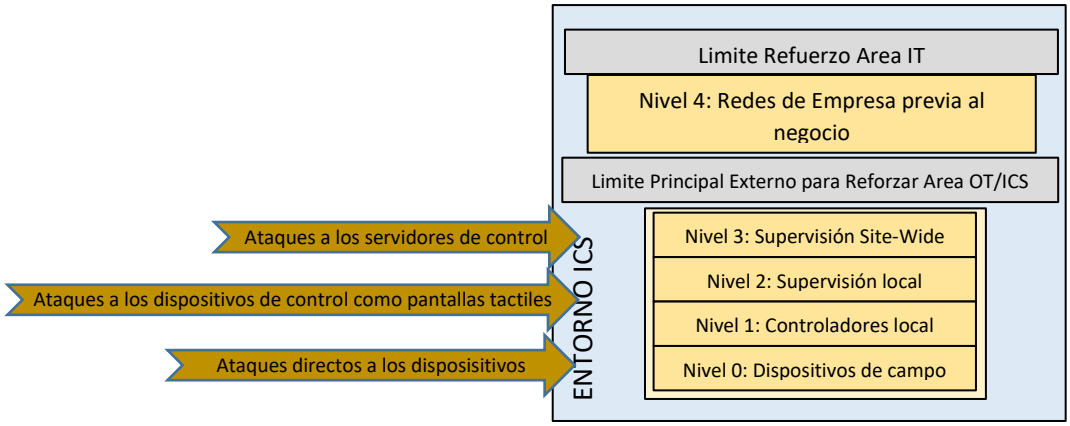


Figura 3 .- Superficie de ataque de la red de control

Dadas las distintas opciones posibles de atacar un sistema, se plantea la estrategia de *árbol de ataque*. Este árbol de ataque organiza de forma lógica las distintas formas de ataque a objetivos pequeños para conseguir uno final mayor, haciendo uso de las distintas vulnerabilidades disponibles en el sistema. Este ejercicio permite igualmente a la organización identificar las debilidades del sistema y los puntos donde la actuación necesaria para garantizar la seguridad es más urgente.

Los arboles de ataque se caracterizan por:

- ser subjetivos, pues dependen del que los hace, de su conocimiento, de su experiencia y de su perspicacia. Normalmente se enfocan a un solo riesgo
- se pueden hacer de abajo a arriba (del objetivo último y principal para el atacante a la primera vía de acceso al sistema que éste utiliza) o de arriba a abajo.
- la búsqueda de un árbol con las suficientes opciones valoradas en el tiempo necesario para implementar lo posible. Este es el aspecto mas importante, pues una evaluación excesiva del sistema puede suponer una respuesta ya fuera de tiempo y un estudio insuficiente puede suponer unas conclusiones ineficaces ante ataques.

Conforme al estudio que se haga se obtendrán unas vulnerabilidades explotables. Las vulnerabilidades son las debilidades del sistema que se pueden explotar por una amenaza, aunque si no hay amenaza la debilidad no es tal. Vulnerabilidad y amenaza forman un tándem de conceptos íntimamente relacionados.

Las vulnerabilidades se ponen de manifiesto con las amenazas que ponen en riesgo el sistema, y estas amenazas y vulnerabilidades pueden ser de muchos tipos: software, de configuración, física, de (falta de) concienciación de la organización, etc. Estas vulnerabilidades son muchas y muy variadas y se registran por las distintas comunidades que velan por la seguridad de los sistemas. Aunque las listas de vulnerabilidades mas comunes son las de IT (www.mitre.org, organiza las vulnerabilidades categorizadas por el CWE o *Common Weakness Enumeration*; organizaciones como

nvd.nist.gov/vuln/search o www.cvedetails.com que organizan las vulnerabilidades por sistemas), también las hay para OT, con sitios específicos de comunidades de SCI a tal efecto. Para SCI el *DHS National Cybersecurity and Communications Integration Center (NCCIC)* es el principal órgano a tal fin. Su programa ICS-CERT va incorporando las últimas vulnerabilidades en SCI y/o brechas de seguridad asociadas (http://us-cert.cisa.gov/ics)

Además de las vulnerabilidades técnicas existe la posibilidad de que un sistema de control industrial esté expuesto a Internet por error, omisión o necesidades del servicio o negocio en cuestión. Esta exposición de un sistema por la razón de que sea la convierte en posible objetivo de explotación de vulnerabilidades. Existen varios métodos para localizar estos sistemas "expuestos" en Internet:

- escaneo activo con herramientas como *nmap* o similar para búsqueda de puertos abiertos, servicios disponibles, etc.,
- análisis de la huella digital en buscadores como Google de una determinada organización o empresa por sus paginas web (haciendo búsquedas orientadas a términos clave como *login*, *passord*, etc. o incluso con áreas específicas como https://www.exploit-db.com/google-hacking-database); o la verificación de sistemas abiertos en páginas y sistemas que están constantemente buscando en Internet estos sistemas(shodan.io que recoge información constantemente de todo tipo de protocolos y no solo HTTP HTTPS, https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting)
- análisis de la imagen en Internet y fuera de ella de la organización, de forma que se verifique la información disponible para cualquier atacante y lo vulnerable que hace a los sistemas que tiene. Así por ejemplo, y sin necesidad de tener a nadie dentro de la organización, puede ser fácil saber qué servicios se ofrecen, desde que IP's, los nombres o datos (email) de personal específico de la organización vinculado, las características de un sistema con ver la definición del puesto de trabajo del operador en cuestión, la información de una solución tecnológica implica conocer sus debilidades, etc.

La superficie de ataque de los sistemas de una organización (y por tanto de la organización en si) debe gestionarse como un recurso más para garantizar la mínima exposición al riesgo. La gestión de la seguridad en SCI y del negocio deben establecer una política de seguridad y fijar los requerimientos a lo que adaptar lo que se exponga al exterior: que información publicar y a quien, que información se ha expuesto en el pasado y catalogarla convenientemente, etc.

Por ultimo debe contemplarse el factor humano para la gestión de la superficie de ataque. La concienciación del personal de la organización es fundamental pues la operación, administración, instalación etc. debe hacerse con una implicación en la seguridad en cada una de sus acciones. Asimismo, generar una base de conocimiento es fundamental para un sistema de gestión concluyente y consistente.

6.1.2. Arquitecturas SCI seguras

En cualquier SCI es primordial tener un frente defensivo, es decir, una red de defensa. Esta red de defensa debe contar con principios básicos como una segmentación adecuada, unos perímetros perfectamente establecidos, configurados y controlados, etc. De hecho lo normal es diferenciar la red de negocio y la de control dado que los sistemas de control tienen más riesgo de ser atacados por ser mayor el impacto que a través de ellos se consigue para comprometer a una organización. Cuanto mejor sea la defensa establecida en el perímetro mejor pero no se debe quedar ahí, y se deben incorporar niveles y separaciones con mecanismos de control para dar mayor seguridad.

Se recomienda que se organicen los sistemas (equipos y redes) por niveles. El modelo de referencia más utilizado es el modelo generado por la universidad de Purdue, y del que ha derivado el que finalmente se recomienda con carácter general: el modelo de la norma ISA/IEC 62443.

Esos niveles reflejan una organización jerárquica de los SCI y de las redes que los interconectan, yendo desde el nivel más bajo (*Level* 0) que sería lo más cercano al campo, al producto, al servicio, etc.; hasta las redes de negocio (*Level* 5). Cada nivel tiene componentes, servicios y funciones, y además puede tener varias subredes.

En los límites entre los niveles es donde se puede poner, aunque no únicamente, la seguridad o la defensa de la red. Las estrategias serían reforzar los límites de cada nivel limitando las comunicaciones entre ambos lados y monitorizar y grabar las que se permitan. Se usan técnicas varias como:

- limitar los niveles: firewalls (físicos y de aplicación), *routers*, ACL, pasarelas y diodos, etc.

- monitorizar los niveles: NIDS&NISP (Sistemas de Detección de Intrusión en Red y de Prevención); NBAD (Detección de anomalías en el comportamiento de una red).

6.1.2.1. Niveles 4 y 5

Purdue Level 5: Enterprise Business Network, o red de negocio de la organización. Es la red con las aplicaciones corporativas que soportan el negocio de la organización. Se suelen incluir puntos de acceso a internet, servidores de correo, servidores web para dar visibilidad y acceso a la organización desde fuera, sistemas CRM, HR, estructuras de directorio corporativas o de gestión documental e incluso acceso remoto por VPN.

Purdue Level 4: Business Network at the plant, o red de negocio de la planta. Suele contener los servicios IT para las instalaciones locales, la unidad de negocio o similar. Se trataría de impresoras, centralitas telefónicas, réplicas locales del directorio, soluciones locales de acceso remoto, etc. donde se reúnen los eventos de seguridad para luego enviarlos, las maquinas con acceso al correo, el acceso a internet, etc. y por lo tanto los empleados de OT

tendrán una estación para acceder a la información de este nivel y otra para OT o permeabilidad entre niveles, sometidas a la seguridad pertinente.

6.1.2.2. Perímetros de seguridad

Cualquier entorno SCI seguro requiere una zona desmilitarizada (DMZ) que se define por sus fronteras con el nivel superior (Purdue Level 4/5, de negocio) y con el nivel inferior (Purdue Level 3: supervisión de planta o fabrica *site-wide*).

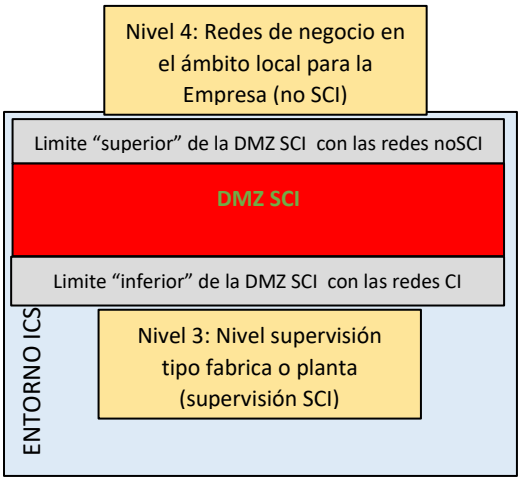


Figura 4 .- Superficie de ataque de la red de control (NIST.SP. 800.82)

Simplificando se podría pensar en un firewall en cada frontera con un nivel Purdue con la DMZ de manera que en ningún caso se permitía el paso de forma directa, sino pasando por algún elemento de dicha DMZ. También se podría hacer con un solo firewall de tres conexiones: una a cada nivel Purdue y otra a un sistema de control de la DMZ. Esta solución supone que el firewall lo gestiona el lado de control del sistema, es decir, el personal de SCI. El debate sobre si es mas seguro el firewall único se basa en el convencimiento de que el sistema de control de la DMZ es mas seguro y menos probable que se vea comprometido que los dos firewalls. Y para este debate los equipos de seguridad de las organizaciones suelen estar en conflicto y se suele optar por que los del lado negocio controlan su firewall y los del lado SCI controlan el suyo, que pueden ser de fabricantes distintos además.

La zona desmilitarizada de los SCI, que llamaremos por su acrónimos en inglés ICS DMZ, puede ser:

- una o varias DMZs,
- mono o multipropósito,
- unidireccional o bidireccional
- etc.

El objetivo será monitorizar todo el tráfico entre niveles y prevenir posibles ataques como el establecimiento de túneles entre los niveles de negocio y los

de control (SCI). Unas prácticas comunes son el evitar usar proxys que den paso directo de datos de un nivel a otro o poner servidores de actualización o herramientas de ciberseguridad en la DMZ.

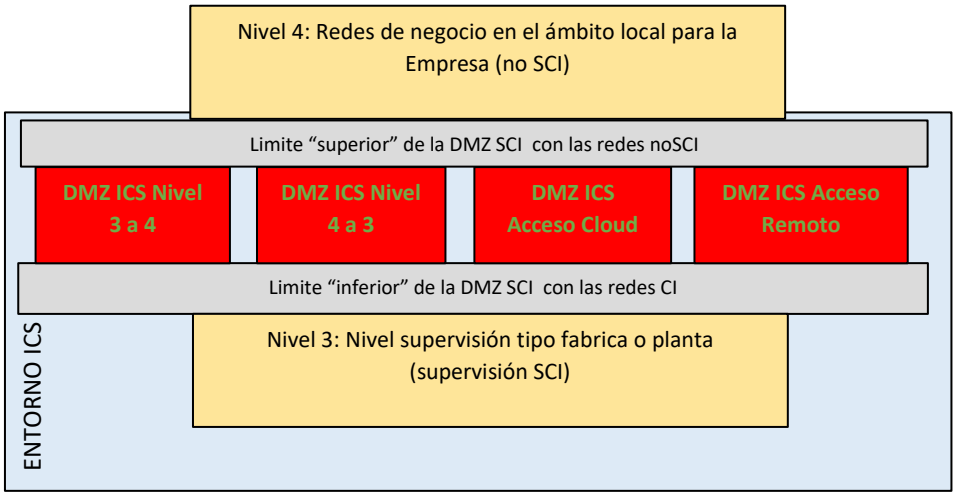


Figura 5 .- Superficie de ataque de la red de control (NIST.SP. 800.82)

6.1.2.3. Nivel Purdue 3: Supervisión a nivel de planta

El nivel 3 engloba funciones de gestión del entorno de operaciones a nivel de planta o emplazamiento de una industria distribuida.

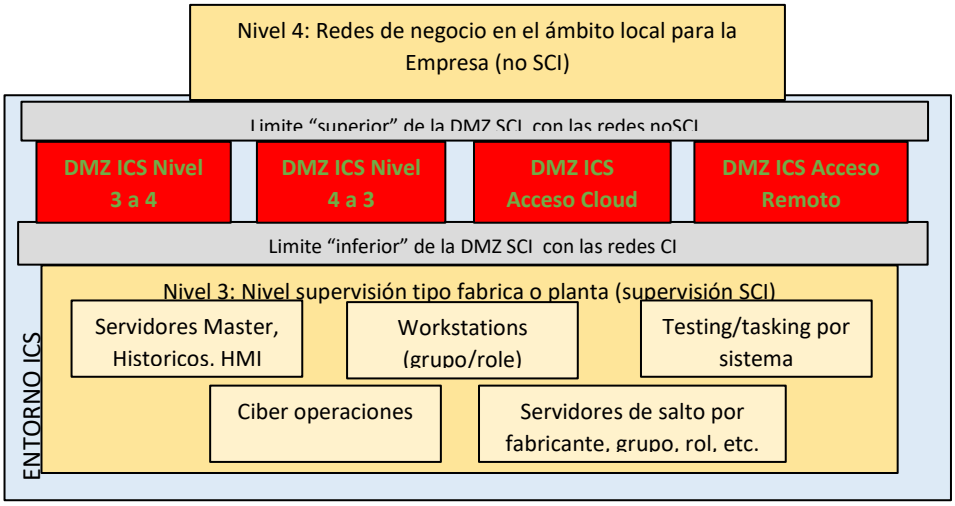


Figura 6 .- Purdue Nivel 3

Se manejan servidores de gestión que actúan:

- dirigiendo operaciones que implican toda la planta,
- sistemas SCADA implantados en el edificio, emplazamiento, célula o similar;
- servidores de alarmas a nivel de toda la planta,
- gestores de alarmas que envían históricos en lugares de la DMZ donde solo se puedan leer y no modificar

- gestores de recursos y planificación de los mismos
- herramientas de fiabilidad y eficiencia en los procesos
- herramientas de modelado y simulación,
- herramientas de análisis de contingencias
- herramientas de visualización
- etc.

La gestión de todos los sistemas tanto de la red de operaciones como SCI, incluyendo el equipamiento de red, el *Active Directory* y los servidores de virtualización deberían estar aparte de lo que haya para el resto de la empresa, del entorno de negocio y estar totalmente controlado desde las redes de operación o SCI. Además las conexiones remotas a los sistemas SCI, independientemente de su proveedor, deben ser a través de la DMZ e incluso de manera no simultánea.

Para ir a más, se puede incluir un área de ciber operaciones o ciberseguridad dentro del nivel 3 como una solución SIEM, un servidor de actualizaciones o sw siempre que esté aislado del exterior. De esta manera se previene a esta área segura y sus datos sensibles de acciones de explotación de vulnerabilidades (ex filtración de datos, control remoto de máquinas, etc.). Se suele utilizar *ACL´s* que independicen la subred ciber de otras subredes del nivel 3. Las tendencias y recomendaciones han pasado de situar estos elementos de ciberseguridad en la DMZ ICS a situarlos en el nivel de control operacional, Nivel 3. Situar estas capacidades ciber (que se conectan a ICS) en la DMZ ICS fuerza a que los firewall dejen pasar directamente desde la DMZ al entorno SCI. De hecho, en el mundo IT tampoco se dejan estas herramientas ni las de actualización en la DMZ pues solo tendría sentido si lo que se quiere es que desde Internet se tuviese la capacidad de gestionar los parches en los servidores internos, algo contrario totalmente a las buenas prácticas en seguridad.

6.1.2.4. Nivel Purdue 2: Supervisión local

El nivel 2 se refiere a la operación y control de los sistemas en tiempo real que sean un solo proceso o grupo lógico de procesos, o una solución DCS, o una línea o célula de producción. Los elementos que suelen tenerse son:

- *workstations* de operación de una sala de control,
- HMI
- *workstation* de ingeniería
- concentradores de eventos de seguridad
- sistemas de alarma en sistemas o procesos
- interfaces directas de comunicaciones
- históricos de datos
- *workstations* de ingeniería o de administración de aplicación o de red específicos de una línea de fabricación o del proceso o la célula

- elementos propios de separación con el Nivel 3
- etc.

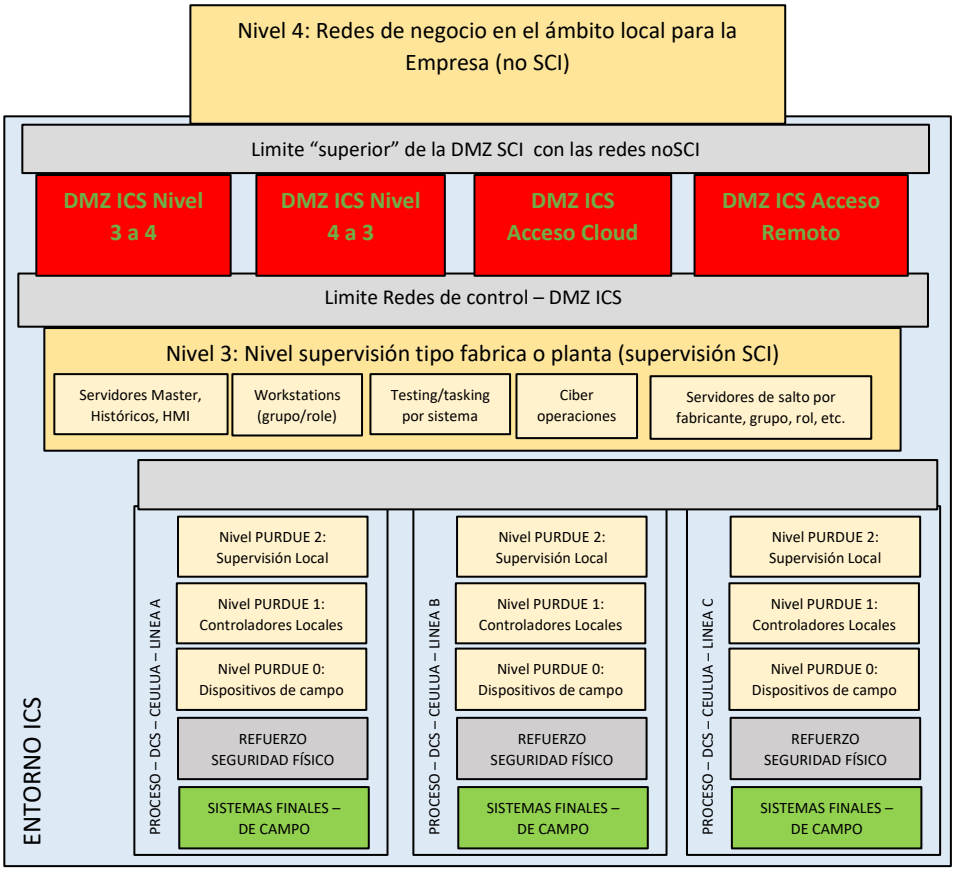


Figura 7 .- Purdue Nivel 2

6.1.2.5. Niveles Purdue 1 y 0

El nivel 0 se refiere a los elementos para el paso del mundo físico al ciber y al revés. Comprende los dispositivos de campos tales como:

- sensores y actuadores de una celda, línea o proceso,
- sensores y actuadores físicos,
- motores y sistemas de automatización,
- dispositivos sensores/actuadores inteligentes,
- instrumentación de campo,
- dispositivos de red de campo (redes entorno industrial),
- etc.

El nivel 1 se refiere a los elementos de los entornos de operación de un lugar específico, como por ejemplo:

- *workstations* dedicadas de operador,
- *PLC´s*
- procesadores de control,
- *relays* programables

- RTU (Unidades de control remoto)
- microcontroladores específicos de un proceso
- etc.

6.1.2.6. Acceso remoto

El acceso remoto a sistemas tiene especial relevancia en estos entornos por ser tan necesario como susceptible de ser vulnerado.

El acceso remoto por parte del personal técnico a los SCI debería hacerse superando dos niveles de seguridad:

- una VPN a la DMZ ICS
- un acceso remoto desde aplicaciones a tal efecto (RDP/VNC/CITRIX) para la conexión a un servidor en el Nivel 3, con credenciales SCI.

Esta formula evitaría el acceso remoto usando cualquier tipo de SW que no se controla de manera que los servidores de acceso remoto pueden ser configurado desde "dentro" de la organización, en concreto desde los host de salto del Nivel 3. Las políticas de seguridad aplicadas a estos host evitarían la ex filtración de información enmascarada con una transferencia necesaria de información que puede hacerse utilizando los mecanismos frontera establecidos en la DMZ ICS.

En el caso extremo de tener que conectarse desde un ordenador remoto sin pasar por los host de salto, se puede considerar añadir escaneo adicional en el momento de su interconexión por VPN, con tratamiento específico por IP o puerto.

6.1.2.7. Conectividad a la nube y al IoT industrial (IIoT)

La nube está cobrando cada vez más importancia en el mundo OT e ICS. En los conceptos como Industria 4.0 o *Smart Grid* se integran cada vez más necesidades de conexión y dependencia nube-SCI, así como gestión de cantidades de datos cada vez mayores tanto dentro del entorno OT como fuera y transitando entre las partes.

La conexión a la nube debe valorarse de manera minuciosa por el impacto que ello tiene en la seguridad. Hay que asegurarse que dicha conexión es necesaria para obtener los objetivos del negocio y cómo afecta a la seguridad, la eficiencia, la eficacia, etc. Y una vez que la necesidad esta asegurada hay que minimizar el impacto del compromiso al que somete dicha conexión a la red del SCI.

La interconexión a la nube supone la presencia de ataques a nuestra red tanto IT como OT, pasando a la red ICS si se puede. Lo primero que hay que pensar es en una DMZ especifica para acceder a la nube (Cloud DMZ) que aísle mediante un firewall específico todo lo que entre y salga de la nube a la red ICS, que limite las comunicaciones del servidor con los dispositivos o sistemas específicamente necesarios y no otros, previendo posibles movimientos laterales entre los elementos de un nivel muy bajo.

Uno de las principales razones para la conexión a la nube es dar acceso a redes de sensores o dispositivos de bajo coste desplegados como una red de micro elementos de poca inteligencia y dando lugar a la IIoT. Parece tanto más interesante una aplicación en la nube cuanto mayor es el número de dispositivos de campo al que tiene acceso, pero eso obvia el factor de inseguridad que supone el disparar el número de dispositivos no-seguros conectados. La idea recomendada por muchas fuentes es considerar una solución IIoT como un proceso único y tratarlo como aislado del resto y securizarlo de igual manera.

6.1.2.8. SCADA Regional

Cuando un SCI se expande más allá de una planta o lugar a lo largo de una ciudad o región geográfica y necesita ser gestionado de manera conjunta el modelo Purdue se complica, aunque puede interpretarse conforme a la siguiente figura.

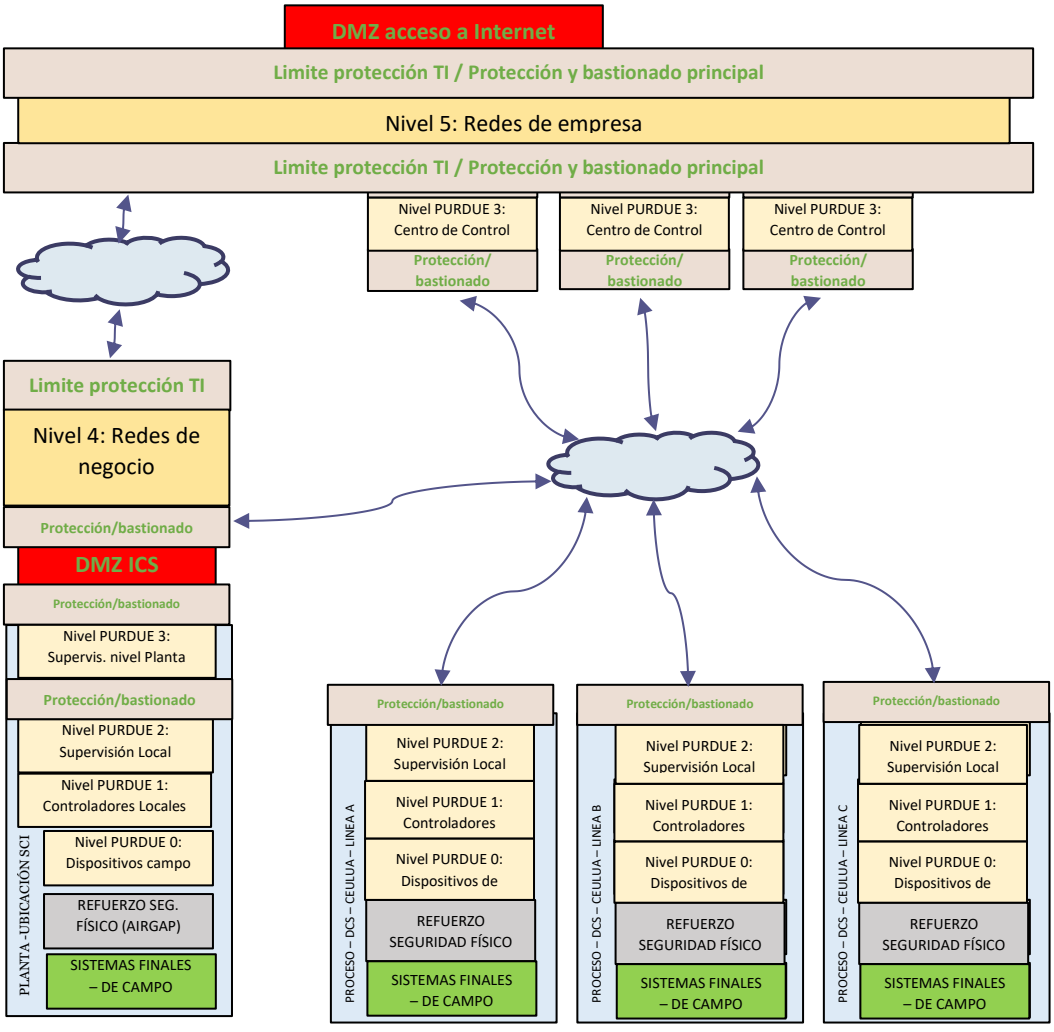


Figura 8 .- Sistema WAN Regional SCADA

Se trata de extrapolar el nivel 3 de Purdue que hasta ahora controlaba a una planta a la región geográfica que englobe las plantas o industrias que

queremos supervisar de manera conjunta. Así los centros de control de SCI, los centros de datos serían Nivel 3 Purdue.

En esa línea, cada lugar remoto distribuido por el área a considerar tal como fábricas, subestaciones, etc. se pueden considerar como procesos, líneas o celdas, cada uno con sus niveles Purdue 0,1 y 2. Se conectarán mediante una WAN para ese SCADA con los centros de control mediante VPN que garanticen la seguridad en el tráfico de control y supervisión que circule por esa WAN. De hecho es en ese tráfico donde es más probable que se produzca un ataque a la infraestructura SCADA ya que transita por lugares de fácil acceso, por empresas de terceros (operadores de telecomunicaciones), etc. y por esto es necesario soluciones de ciberseguridad basadas en criptografía que hagan el descifrado difícil y el ataque o la detección de sistemas más complicado.

6.1.3. Ataques a nivel PURDUE 0 y 1

6.1.3.1. Superficies de ataque a nivel Purdue 0 y 1

Los elementos más comunes de estos niveles y que normalmente llamamos controladores, tales como PLC´s, (*Programmable Logic Controler*), RTU (*Remote Terminal Unit*), IEDs (*Intelligent Electronic Devices* típicos de la industria de la energía) son en sí mismos una gran superficie de ataque para los que hay que desarrollar una estrategia común de defensa.

De forma general consisten en una CPU, memoria (ROM con la información necesaria para ejecutar lo almacenado en RAM y otros registros donde también vuelcan el resultados de las operaciones que se requieran), puertos de interconexión al dispositivo e interfaces de entrada y de salida para la interacción con el exterior.

La superficie de ataque a este nivel se refiere:

- a componentes físicos como chips, tarjetas, puertos varios (RS232, SD-card, USB, etc.). El acceso a través de cualquier puerto permite inyectar malware que puede actuar en cualquier parte del dispositivo, y mas cuando son interfaces desarrollados e incluidos en el diseño para probar el dispositivo, darle mantenimiento y en general cualquier fin en el que no se incluye la seguridad en su diseño (mecanismos de control de acceso o autenticación).y el acceder a ellos es tan sencillo como quitar la tapa que los protege. El acceso físico a los dispositivos abre un abanico de posibilidades al que debe incorporarse la posibilidad de acceso en su proceso de transporte, almacenamiento, instalación o puesta en marcha, normalmente sometido a menos exigencias que elementos IT. Normalmente los dispositivos de este nivel presentan interfaces en si mismos (directo como un teclado, una conexión para uno, etc.) para mantenimiento, detección de averías o programación directa. Dichos interfaces no suelen tener control de autenticación y si lo tienen se pueden evitar con facilidad, y mucho mas si los valores configurados son los valores

mas comunes (user/password https://github.com/hackingyseguridad/diccionarios)

- al firmware/RTOS de los dispositivos, explotando sus vulnerabilidades que como sistema operativo en tiempo real pensado para un dispositivo de bajas capacidades no incluye consideraciones como evitar cuentas por defecto grabadas en el HW, usar autenticación fuerte, evitar envío de tráfico en claro en transacciones FTP o Telnet (que ciertamente no tenía previsto en su diseño inicial el cifrado de tráfico como requisito), evitar el depurado de código que permita desarrollar procesos de ingeniería inversa o bien lecturas/escrituras no autorizadas o sin autenticación. Asimismo, y apoyándose en el acceso a datos, código y lógica, pero sobre todo en ausencia de los mecanismos mencionados u otros como la verificación de integridad de código o información da lugar a que cualquier acceso por el *backplane* del dispositivo o por módulos Ethernet cada vez mas comunes sea una brecha de seguridad de gran importancia. La principal medida para este ataque es prevenir el acceso directo a los puertos de comunicación o el dispositivo en sí, proteger las comunicaciones que utilicen ese firmware para evitar inyección de código, por ejemplo.

- a las aplicaciones que tengan los dispositivos, que cada vez mas incluyen servidores web para mostrar la información y con ellos sus vulnerabilidades.

- a las comunicaciones entre los dispositivos y con el servidor correspondiente de alarmas, de ingeniería, de gestión, etc. que suelen tener muy pocas capacidades de seguridad y de hecho suelen no autenticar el origen de los datos, facilitar los accesos desde la red de negocio de la organización, utilizar una red plana sin segmentar por *VLANs* o utilizar los mismo servicios de red en la parte de negocio y en la de operación. Otra forma de obtener ventajas sobre un sistema apoyándose en la comunicaciones es explotando las vulnerabilidades de las claves de cifrado (que suelen ir en comunicaciones, pero no solo en éstas) y el estudio de su aleatoriedad y en la entropía que presenta.

- a la gente que manipula, transporta, instala, pone en marcha y, por último, opera los dispositivos directamente en la planta. y que actúa de manera maliciosa o simplemente despreocupada por algo como la seguridad

6.1.3.2. Dispositivos inteligentes (Ej. *Smart Meters*)

Los dispositivos inteligentes, cada vez mas presentes aunque con capacidades limitadas sean *legacy* o no, son tan fáciles de atacar como cualquier otro y de hecho es tanto mas vulnerable cuanto mas inteligente es a pesar de lo que se pudiera pensar pues su inteligencia esta normalmente asociada a capacidades de operación pero no incorpora funcionalidades de seguridad.

6.1.3.3. Ataques a los servidores de gestión y HMI desde dispositivos en planta

Los elementos de nivel Purdue 0 y 1 pueden permitir el acceso a atacantes cuyo objetivo es el servidor de gestión instalado en niveles superiores. En concreto son las RTU (*Remote Terminal Unit*) las que están en constante comunicación con estos servidores, cuyos protocolos se pueden atacar como cualquier otro.

Atacar un RTU permitiría una vía de acceso "hacia arriba" para llegar al servidor de gestión e implementar una denegación de servicio (DoS), una ejecución de código en el *gateway* o en el microprocesador del *front-end* para así acceder a la red de control.

6.1.4. Tecnologías de nivel PURDUE 0 y 1

6.1.4.1. Tecnologías de elementos de campo o de planta

Los dispositivos de que se dispone a nivel de planta en un entorno industrial o de campo son de lo más variados y sus orígenes y naturaleza tecnológica también.

La naturaleza de uso, no solo la tecnológica, condiciona tremendamente la seguridad para estos dispositivos. El resultado es una panoplia de dispositivos y características de seguridad; fórmulas de acceso; usuarios, técnicos y operadores de sistemas y dispositivos; labores de mantenimiento (actualizaciones de software/firmware, calibración, etc.); variedades de impactos posibles, etc. complicado de gestionar para dar lugar a una seguridad que, por definición, nunca llega a ser total.

Un aspecto reseñable y relevante es el SW de que disponen los dispositivos en sistemas de control industrial. Dichos dispositivos, por su simplicidad, cuentan con el SW indispensable para la labor para la que están diseñados, sin contar con sistema operativo. En los casos más complejos, como sistemas empotrados o embebidos, tienen sistemas operativos simplificados al máximo y donde, como normal general (y de ahí le viene el nombre) la respuesta en tiempo real es la prioridad para una integración en un sistema mayor, evitando sistemas de propósito general y el SW asociado donde ofrecer una variedad de servicios puede ser la prioridad. Para estos sistemas operativos en tiempo real RTOS[2] resulta especialmente de interés el control de los ciclos de CPU para una respuesta a o de un proceso o bien ante una entrada o para proporcionar una salida.

Los dispositivos que cuentan con RTOS y arquitecturas sencillas son tan vulnerables como difícil es conseguir la especialización necesaria para

[2] Un sistema operativo en tiempo real (RTOS) es un sistema operativo ligero que se utiliza para facilitar la multitarea y la integración de tareas en diseños con recursos y tiempo limitados, como suele ocurrir en los sistemas integrados. Además, el término "tiempo real" indica previsibilidad/determinismo en el tiempo de ejecución más que velocidad bruta, por lo que normalmente se puede demostrar que un RTOS satisface los requisitos de tiempo real duro debido a su determinismo. (RTOS, s.f.)

conocer sus principios de funcionamiento y diseño, sus vulnerabilidades y cómo explotarlas. No obstante, por su simplicidad, si se cuenta con lo necesario, una vez se accede al dispositivo, las capacidades e información totales se ven comprometidas sin otras figuras que permitan encadenar vulnerabilidades (pivotaje o *hooking* por ejemplo).

La importancia del tiempo es también extensible a la sincronización de los distintos elementos, a su control y al registro de acciones (logs), por lo que no solo hace falta una referencia fiable como sistemas de navegación globales basados en satélites (GPS, GLONASS, GALILEO, etc.) sino una infraestructura y protocolos de sincronización (Network Time Protocol, Precisión Time Protocol, etc.) para cada todos los elementos de un sistema SCADA. Cada fuente (por ejemplo las proporcionadas por NIST https://tf.nist.gov/tf-cgi/servers.cgi) tendrá una fiabilidad, estabilidad y características que condicionará la clasificación del sistema que de ella se sincronice y cómo se sincronice.

6.1.4.2. Protocolos para dispositivos de campo o de una línea de producción

Un protocolo estandariza una comunicación entre partes, dicho sea esto de manera amplia y sin entrar en división por funcionalidad, elementos, nivel, etc.

Los protocolos para interconexión de elementos de campo tradicionalmente se implementaban en un bus serie que unía dichos elementos y cuyas características eran conseguir comunicaciones en tiempo real (determinísticas), fiables independientemente del entorno (normalmente hostil por el nivel de ruido, suciedad, interferencia, etc.) y seguro (desde el punto de vista de la operación de los sistemas).

Los protocolos tradicionales han tenido que evolucionar para permitir mayor interoperabilidad entre fabricantes, mayor complejidad de terminales y sus comunicaciones, más agilidad y menor latencia y, por último, introducir capacidades de ciberprotección. Esta evolución ha sido fruto de una convergencia entre los protocolos industriales y los de redes de TI como Ethernet o TCP/IP[3].

La implementación de la comunicación se hace mediante módulos al efecto que se adaptan al dispositivo y al medio de transmisión. Incluso hay elementos como por ejemplo un *gateway* que permite la adquisición de datos de varios elementos y su transmisión por el protocolo que sea y el medio de que se disponga (fibra, *wifi*, gsm, etc.).

3 Ejemplos de protocolos son FOUNDATION Fieldbus, CIP (Common Industrial Protocol) , PROFIBUS and PROFINET, P-NET (Process NETwork), FIP (Factory Instrumentation Protocol) , INTERBUS – CC-Link (Control and Communication), HART (Highway Addressable Remote Transducer), EtherCAT Ethernet Powerlink, EPA (Ethernet for Plant Automation), Modbus, CAN bus, IEC 61850, etc.

6.1.5. Defensas de nivel PURDUE 0 y 1

La fiabilidad en la operación de sistemas de control industrial está referida a garantizar su funcionamiento ante un fallo, lo que en términos anglosajones se considera como *safety*

La inclusión en los requerimientos de cualquier sistema de medidas específicas de fiabilidad es cada vez más frecuente, tanto con pruebas de verificación durante la fabricación del dispositivo, como al instalarlo en el sistema industrial que sea.

La mejor forma de lograr unos niveles 0 y 1 fiables es definir claramente los requisitos que tienen que cumplir, obtener la certificación del fabricante del cumplimiento de esos requisitos, dar robustez al sistema, aumentar el control y monitorización e igualmente los sistemas de seguridad y control de calidad.

Se ha desarrollado un lenguaje de especificación de requisitos que reduzca las ambigüedades al definir un sistema o un dispositivo, unas pruebas de conformidad con normas de fiabilidad y seguridad e incluso un programa certificado por ANSI (ISASecure) para certificar a su vez PLCs y dispositivos de campo de sistemas de control industrial.

Por último cabe señalar en este punto los sistemas de seguridad tanto para las personas como para los sistemas (*Safety Instrumented Systems*). Estos sistemas, asociados a los elementos críticos, suelen ir separados del sistema de control industrial y se plasma en elementos tales como detectores de humos, botones de parado, etc. La seguridad perseguida es la asociada al acrónimo SH&E (*Safety, Health & Environmental*) y el proceso industrial debe siempre mantenerse dentro de los umbrales de seguridad que se establezcan. Dichos umbrales se apoyan en la distinta normativa, dependiendo del ámbito de la industria siendo la IEC61508 la más genérica de todas para diseño construcción y operación de sistemas eléctricos, electrónicos y de electrónica programable (exida.com, s.f.).

Al final se genera un "estudio de peligro y operabilidad" (*HAZard and OPerability HAZOP study*) donde se definen los niveles de seguridad integral (SIL - *Safety Integrity Levels* de 1 a 4 según sea menor o mayor riesgo) para un SIS y se mide la probabilidad de fallo de un sistema (crossco.com, s.f.)

Frecuencia						
	5	SIL3	SIL4	X	X	X
	4	SIL2	SIL3	SIL4	X	X
	3	SIL1	SIL2	SIL3	SIL4	X
	2	-	SIL1	SIL2	SIL3	SIL4
	1	-	-	SIL1	SIL2	SIL3
		1	2	3	4	5
		Severidad De La Consecuencia				

Tabla 1 .- Niveles de seguridad SIL – Matriz HAZOP

Los subsistemas de seguridad que antes eran independientes han pasado a estar integrados en el sistema que protegen, por principios de economía de medios, proximidad al parámetro a considerar, etc. (Siemens, s.f.) (DesignNews –, s.f.). Estos subsistemas son susceptibles de ser atacados y configurar una zona de la superficie de ataque (Fireeye.com, 2017)

6.2. COMUNICACIONES Y PROTOCOLOS

Los protocolos mas utilizados en IT desde nivel 2 a 4 de la torre OSI (TCP/IP y ETHERNET) se han extendido a OT, haciendo posible una convergencia de las tecnologías y desarrollos a más alto nivel entre ambos mundos, una ampliación en la fabricación de dispositivos y sistemas complejos, una capacidad de interrelación entre ellos, etc.

Como resultado del uso de estos protocolos, los conceptos de sobra conocidos y que en principio no correspondería mencionar en este trabajo, son de obligado repaso pues van a permitir el uso de *hubs*, *switches*, bridges, routers, etc. en sistemas industriales, con las adaptaciones que correspondan para aplicar de la misma manera estructuras de seguridad equivalentes (VLANs, ACL´s, NAC´s, etc.).

Toda vez que se ha recalcado la importancia de estos protocolos de comunicaciones, cabe señalar varios aspectos relevantes en su relación con sistemas de control industrial:

- Los protocolos ICS pueden adaptarse a los protocolos “IT” a partir de nivel 3, aprovechando las capacidades de direccionamiento y enrutamiento TCP/IP, aunque no siempre es así. Existen implementaciones de protocolos ICS sobre Ethernet, optimizando la eficiencia al no tener que tratar las cabeceras TCP, por ejemplo, minimizando la latencia, etc. Ejemplos de estas implementaciones son *Foundation Fieldbus High Speed Ethernet* (HSE), *PROFINET* (RT, IRT), *CC-Link IE* (Control, Field, Safety), *EtherCAT, MECHATROLINK-III, IEC 61850 Goose and Sampled Values* (SV), etc. Estos protocolos cuentan con las características de ICS: soporte de procesos determinísticos, conectorización rugerizada, etc.
- Cualquier dispositivo en una red IT se va a identificar, como poco con dos direcciones (MAC a nivel 2 e IPv4/IPv6 a nivel 3) y un nombre. Las filosofías, los riesgos que comportan, etc. cuando se aplican a OT se trasladan a los SCI aunque con ciertas peculiaridades. Así por ejemplo, no se soporta IPv6. Hay multitud de protocolos adaptados, que según sea para un entorno u otro se pueden poner distintos ejemplos (Wikipedia, 2022) , incluso con el puerto asociado:

    - Gestión de dispositivos de planta/campo *(Fieldbus Management)*
        - EtherCAT: UDP/34980
        - EtherNet/IP: TCP/44818, UDP/2222,44818

        - FL-net: UDP/55000 a 55003
        - FOUNDATION HSE: TCP/1089-1091, UDP/1089-1091
        - HART-IP: TCP/5094, UDP/5094
        - PROFINET: TCP/34962-34964, UDP/34962-34964
    - Comunicaciones en entornos regionales de un sistema SCADA (*Regional SCADA)*
        - Modbus TCP: TCP/502
        - DNP3: TCP/20000, UDP/20000
        - WITS: TCP/20000, UDP/20000
        - DLMS/COSEM: TCP/4059, UDP/4059
        - IEC 104: TCP/2404
        - IEEE C37.118: TCP/4712, UDP/4713
        - MMS: TCP/102
    - Local SCADA
        - HMI, Históricos y Servidores de Alarmas
            - OPC DA: TCP/135 + TCP/1024-65535
            - OPC UA: TCP/4840
            - OPC UA XML: TCP/80, TCP/443
        - Centros de control SCADA
            - ICCP/TASE2: TCP/102
        - Específicos de automatización de edificios
            - BACnet/IP: UDP/47808
            - LonTalk: UDP/1629, UDP/1628
            - Fox (Tridium/Niagara): TCP/1911

  Todos estos protocolos, o la gran mayoría de ellos, son abiertos para que cualquier fabricante pueda utilizarlos en sus productos que suelen aplicarlos junto con un protocolo propietario o una forma de comunicación entre dispositivos cercanos específicos. No obstante a lo anterior, aunque muchos protocolos no están basados en TCP/IP es muy frecuente disponer de técnicas de encapsulamiento paquetes de este estilo.

- La mayoría de lo protocolos industriales están pensados para el control de sistemas aislados donde la seguridad no es la prioridad, resultando muy vulnerables a ataques MITM o explotar vulnerabilidades derivadas de la falta de protección en los procesos de autenticación o verificación de integridad. Es la norma IEC 62351 (IEC 62351, s.f.) la encargada de llevar la seguridad a protocolos como estos, en concreto a la serie IEC TC 57 (encargados de las normas de comunicación de información en sistemas de energía y sistemas de gestión y distribución de energía). Las recomendaciones mas comunes son la reducción de superficie de exposición física y lógica, la segmentación con control de flujo, diodos de datos, etc., uso de VPN para cifrado, firewalls, ACL´s, uso de firmas para su integración en IDS/IPS, etc.

6.2.1. Ataques y protecciones típicas en redes de ICS

Los ataques y medidas de protección para ellos se pueden organizar pensando en una red con sus protocolos dependiendo del lugar de la pila OSI donde se tenga

una vulnerabilidad y se quiera minimizar su exposición. La captura del trafico de red si se tiene acceso al medio de transmisión utilizado es una técnica frecuente y de gran impacto pues permite acceder a datos relativos a todos los niveles o a partir de los cuales iniciar explotación de otras vulnerabilidades (descifrado de comunicaciones, interceptación de *tokens*, acceso a redes de gestión, etc.).

Los ataques que suelen darse son los de:

- denegación de servicio (por ocupación de ancho de banda disponible, o de recursos del sistema que suelen ser mas limitados que en redes IT; por interferencia en el medio de transmisión, etc.)
- ataques *Man-in-the-Middle* aprovechando la falta de cifrado en las comunicaciones y exponiendo todos los protocolos por encima del nivel físico.
- suplantación de identidad en las señales de control (*Spoofing Control Signals*) apoyándose en lo mismo que en el caso anterior, aunque atacando directamente al dispositivo como elemento gestionado y gestionable.
- *fuzzing* con los protocolos de red, es una técnica de pruebas de software a menudo automatizado o semiautomatizado que implica proporcionar datos inválidos inesperados o aleatorios dentro de un intercambio de mensajes en un protocolo. La introducción de valores inesperados al enumerar los dispositivos o sus capacidades (numero de entradas o salidas de un sensor o actuador), o en una consulta a un campo determinado de una aplicación o espacio software como es el buffer dan una idea de las vulnerabilidades disponibles y es solo cuestión de tiempo y habilidad poder explotarlas.

La mejor protección en un entorno ICS es una red aparte para proteger el control y los datos de dicha red, impidiendo el acceso a la parte de control y llevando perfecta cuenta de los datos que pasan los límites o fronteras de protección del entorno ICS e incluso sus distintas áreas. El modelo Purdue de la norma ISA-95/Purdue recomienda establecer, como mínimo, siguientes límites, zonas o áreas para las redes ICS:

- Zona de sistemas SIS
- Zona de Control básico o Área de PLC´s
- Zona de supervisión o Área de HMI.
- Zona de proceso de información o Área de históricos de datos
- Zona de red IT

Los dispositivos mas comúnmente utilizados para estableces estos límites son firewalls tradicionales y de nueva generación (NGF), sistemas de gestión de amenazas (Universal *Threat* Management UTM) y de detección y prevención de sistemas (Network *Intrusion Detection/Prevention systems* NIDs/NIPs), diodos de datos, sistemas de monitorización de red para detección de anomalías, soluciones de verificación de ficheros y dispositivos USB, *honeypots*, etc. La descripción de estos elementos esta fuera del alcance de este texto, aunque deben

ser mencionados al menos y pensar en dispositivos de redes para IT potenciados para entornos OT.

Los ataques entre niveles a señalar especialmente relevantes son los ataques a los servidores de gestión y HMI desde dispositivos en planta, y de ahí la necesidad de la estratificación y elementos de separación, monitorización y control. Se verá más adelante, pero cabe señalar dos proyectos especialmente relevantes a nivel europeo, que son C4IIOT y SECOIIA[4], donde se hace especial hincapié en la separación por niveles, en su defensa y en los riesgos que se evitan. Estos proyectos están marcando las líneas futuras en muchos aspectos como la Industria 5.0, objetivos comunes, etc.

6.3. SISTEMAS DE SUPERVISIÓN

6.3.1. Ataques a la supervisión

Una parte importante al valorar la seguridad de un SCI y la infraestructura que les incluye es identificar los sistemas de supervisión, lo que conllevan en lo relativo a la seguridad y valorar el riesgo asociado

Los servidores y estaciones de trabajo (*workstations*) se localizan en cualquier punto de la red de control.

Aunque los servidores de gestión están en pocos sitios perfectamente localizados, pueden existir multitud de servidores intermedios en sitios remotos en la red de campo. Todos ellos deben tenerse en cuenta para dar seguridad global. Los servidores centralizados son los que presentan el mayor riesgo por ser los que mas elementos controlan, pero no pueden caer en el olvido los servidores a nivel de campo que presentan un riesgo mayor que cualquiera de los dispositivos que haya en torno a él.

En cuanto a las *workstation*, habrá de éstas por toda la red de control (centro de control, oficinas distribuidas con técnicos de campo, etc. que normalmente llevan un sistema operativo común como Windows o Linux y aplicaciones para la interacción del usuario con el sistema. Pueden ser distintos tipos de equipos, como portátiles, teléfonos, *tablets*, HMIs, etc.

El interés que tiene un atacante en elementos de supervisión reside en varias razones:

- Le resulta mas fácil por usar tecnologías mas comunes:
    - TCP/IP, que es mas conocido que los protocolos industriales,
    - Sistemas operativos como Windows, que son mas ampliamente utilizados y sus vulnerabilidades mas conocidas y explotables y explotadas.
- Se puede acceder desde los HMI a los procesos del ICS de forma directa

[4] C4IIOT - https://www.c4iiot.eu/
SECOIIA - https://secoiia.eu/

- Si se accede a los ficheros de proyecto se consigue una visión información general del sistema
- Se puede conseguir control de alto nivel si se accede a los servidores de gestión

El objetivo principal va a ser en un sistema ICS el software de control que se ejecute en servidores y *workstations*, por lo que debe estar configuradas sus opciones de seguridad y bastionados los elementos donde se ejecutan. Incluso si se utilizan elementos externos que adapten legacy o unos dispositivos a otros o a la red (BTW *Bump*-in-the-*wire*, *proxies*, VPN, etc.) son susceptibles de ser atacados y su configuración de seguridad es prioritaria.

Las técnicas más probables para estos sistemas son la ingeniería social, *spear*/*phising* (sobre los usuarios de servidores y *workstations* o sobre los técnicos de campo)

Un ejemplo de ataque a un sistema de supervisión es *Conficker*, que dio lugar a incidentes sobre redes eléctricas (Conficker Worm – A Worm That Affects Microsoft Windows, 2022), aunque el ataque de referencia es *Stuxnet* (Stuxnet 0.5: The Missing Link, 2013). El ataque a sistemas de supervisión puede no ser específico de redes ICS, por ser redes y sistemas comunes en IT pero la explotación de la información o la vulnerabilidad si requiere de habilidades del mundo OT. Véase el ejemplo de la referencia (Cybersecurity & Infrastucture Security Agency, 2017) donde un servidor web de un sistema SCADA da lugar a una vulnerabilidad en la autenticación de usuarios.

Un resumen interesante de amenazas para ICS en el ámbito de su red de supervisión es el ofrecido por Kaspersky (ics-cert.kaspersky.com, 2021) donde no solo se ve el auge de los incidentes en redes ICS, sino a través de Workstations y laptops de dichos sistemas como vector de entrada y el SW que tienen, aunque las técnicas de ataque son la explotación de la confianza en las relaciones entre las personas y los hábitos de trabajo.

6.3.2. Históricos/historiadores y bases de datos

En los sistemas de supervisión son especialmente interesante las bases de datos, y de ellas los historiadores de datos donde el SCI almacena valores que el sistema global SCADA gestiona a niveles superiores.

La clasificación de las bases de datos se puede hacer atendiendo a dos criterios:

- El criterio temporal de captura, almacenamiento, disponibilidad y uso para el que se tratan los datos, y en tal caso tenemos históricos operacionales o simplemente históricos (o historiadores) de datos:
    - Los operacionales tienen unos requisitos de disponibilidad mayores y disponen de redundancia para tareas críticas. Son históricos que se toman en tiempo real. Son los utilizados por los ingenieros de planta y a menudo este SW se integra o se utiliza junto con los sistemas de control DCS y PLC estándar para

proporcionar capacidades mejoradas de captura, validación, compresión y agregación de datos. (Wikipedia, 2022)

    - Los historiadores almacenan la información que se requiere en la red de operaciones (planificación de mantenimiento y operaciones en si, ingeniería, soporte, etc. mas a largo plazo para optimización de procesos por ejemplo) y en la red de negocio/empresa (contabilidad, planes, etc. que suelen tener copias de seguridad mas a largo plazo y acceso desde mas sitios y de forma remota).

- El punto de las operaciones y procesos desarrollados en el SCI de donde se obtienen o se aportan dichos datos, según:
    - Alimentan a los procesos de las operaciones que son los que implementan el SCI: datos generados en tiempo de ejecución, en tiempo real, con etiquetas y elementos de cada proceso (formulas, fichas de datos, diagrama de estados, etc.)
    - Se recogen de las los procesos desarrollados en las operaciones, y se incorporan a la gestión/mejora de los procesos que están siendo monitorizados y gestionados: historiadores de datos, almacenamiento de alamas, de datos de análisis, eventos y logs varios, etc.,
    - Se usan para configurar proyectos y configurara dispositivos y sistemas: bases de datos de proyecto, de configuración general o específica y esquemas de funcionamiento.
    - Se usan para las aplicaciones de usuario para soporte e interacción con el SCI (desde una sala de control por ejemplo): datos de las instalaciones, de los activos, datos GIS, datos de pronostico y planificación, datos de/para la asignación de tareas, datos de seguridad (SIEM, AV,etc)

La localización de historiadores suele ser en DMZ con elementos de seguridad que garanticen la estanqueidad de las capas o niveles de la arquitectura. Los datos serán requeridos o suministrados desde distintos puntos de la organización y eso se ha de tener en cuenta para evitar caminos indeseados entre niveles.

Hay cuatro categorías de bases de datos en un SCI, dependiendo de si dichos datos:

- Alimentan a los procesos de las operaciones que son los que implementan el SCI: datos generados en tiempo de ejecución, en tiempo real, con etiquetas y elementos de cada proceso (formulas, fichas de datos, diagrama de estados, etc.)
- Se recogen de las los procesos desarrollados en las operaciones, y se incorporan a la gestión/mejora de los procesos que están siendo monitorizados y gestionados: historiadores de datos, almacenamiento de alamas, de datos de análisis, eventos y logs varios, etc.,

- Se usan para configurar proyectos y configurara dispositivos y sistemas: bases de datos de proyecto, de configuración general o específica y esquemas de funcionamiento.
- Se usan para las aplicaciones de usuario para soporte e interacción con el SCI (desde una sala de control por ejemplo): datos de las instalaciones, de los activos, datos GIS, datos de pronostico y planificación, datos de/para la asignación de tareas, datos de seguridad (SIEM, AV,etc)

La forma en la que la información se agrega a los históricos tanto operacionales como de empresa determina una arquitectura propia de cada organización, en función de las capacidades de sus activos en todos sus niveles.

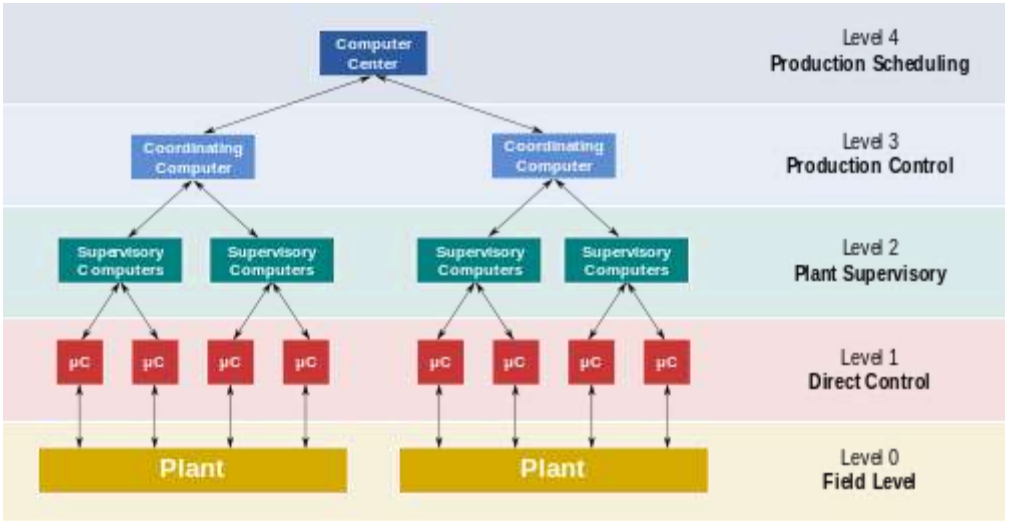


Figura 9 .- Referencia para el almacenamiento de históricos, (en Supervisión).

Así por ejemplo, OSIsoft establece niveles para proporcionar cinco etapas (recolección, almacenamiento, contextualización, visualización y toma de decisiones e integración, compartición y mejora (OSISoft, is not part of AVEVA):

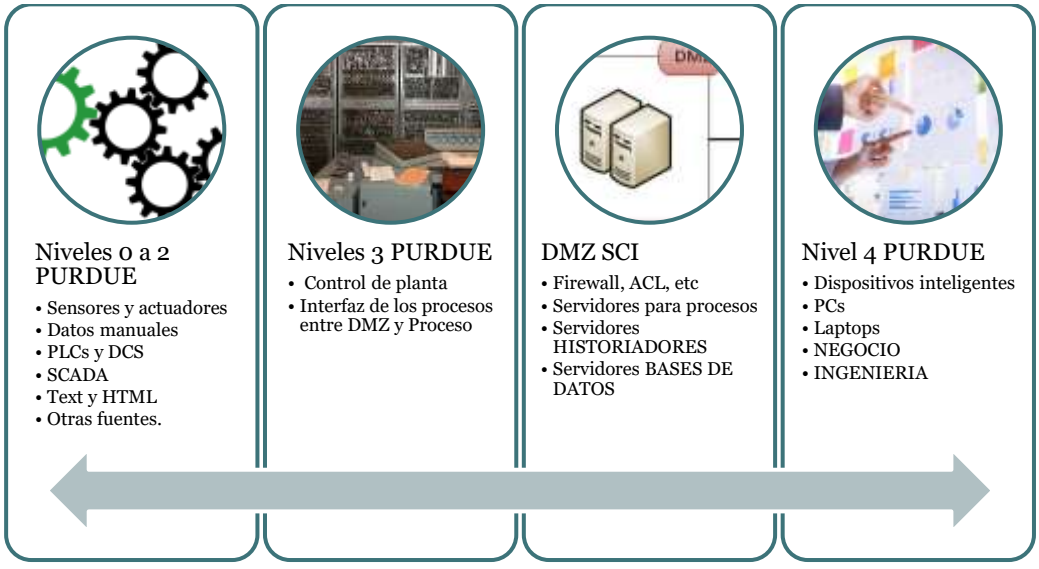


Figura 10 .- Agregar datos a históricos

6.3.1. Historiadores como superficie de ataque y securización

Tal y como hemos visto los historiadores pueden almacenar tanto datos de un proceso de mas bajo nivel (mensajes, medidas, acciones, etc.) como proceso, como de ingeniería, de negocio, etc. Esto supone que la información puede ser de funcionalidad, de usuario, etc. La información que se va a almacenar en un historiador puede ser susceptible de ser modificada para obtener un beneficio o ventaja. Aunque tienden a estar en DMZs en sistemas bastionados, el acceso a ellos es de interés por ofrecer información completa de la organización.

Los vectores de ataque son los ya mencionados mas arriba, dependiendo del elemento del SCI que se vea afectado por un atacante: pares usuario/password por defecto en dispositivos de campo, fallos en la configuración de los protocolos de comunicaciones (especialmente aquellos para conexión remota), etc.

Aun ajustando la seguridad a los historiadores y demás bases de datos suele ser susceptible de ataque los privilegios que se suelen dar en conexiones entre niveles con fines específicos como por ejemplo las que se hacen para *backups* de larga duración (entre DMZs, o DMZ y MZs para servicios, etc.). Se recomienda utilizar interconexión entre niveles PURDUE 3 y 4 para historiadores y aplicaciones que "beban" de ellos de forma dedicada y especialmente controlada.

En cuanto a las bases de datos se recomienda su securización (*hardening*) y bastionado, garantizando configuraciones como usuario/password único para cada aplicación o base de datos, no usar cuentas de administrador de dominio como usuario, evitar llamadas a funciones no sanitizadas, etc. Asimismo resulta prioritario alinear el sistema de administración de base datos con los historiadores en lo que a securización se refiere: *patching* de todas las maquinas y aplicaciones, separaciones de roles y funciones, garantizar el soporte, monitorización de procesos y eventos de seguridad, etc.

6.3.2. Interfaces de usuario

La interfaz de usuario de los elementos de un sistema de control industrial (SCI/ICS) puede ser un interfaz hombre-máquina (HMI) tradicional, uno de ultima generación, individual, integrado en un sistema jerárquicamente superior mediante sistemas padre, etc.

Los HMI, suelen dar acceso al proceso y resulta frecuente encontrar HMI conectados vía serie o por bus de campo (en planta Nivel 2) a los dispositivos, o bien ya a nivel 3 desde interfaces Web a los que se accede por la red de control desde un *front-end* con protocolos que pueden ser específicos, pero cada vez mas son sobre redes IP. Esta tendencia permite el desarrollo de interfaces a los dispositivos con perfil de ingeniería, de administración, de mantenimiento, de análisis, etc. aumentando las opciones tanto de funcionamiento como de vulnerar la seguridad con los ataques típicos web.

Cabe señalar las vulnerabilidades mas comunes conforme a la OWASP (OWASP.ORG, 2022) para remarcar qué supone para un SCI el tener interfaces web para los HMI y otros interfaces

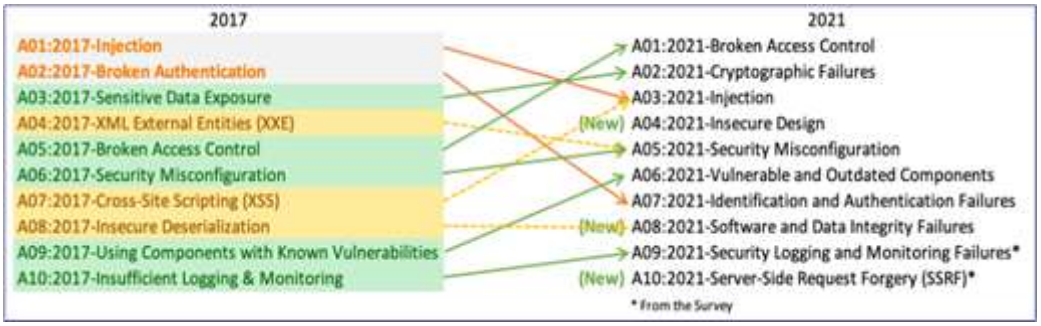


Figura 11.- OWASP TOP 10 web application security risks

Estas vulnerabilidades hay que ponderarlas con las características de los dispositivos del SCI. Así por ejemplo hay sistemas que para las *passwords* tienen restricciones como longitud máxima de 8 caracteres, no se usa *hashing*, solo caracteres alfanuméricos no especiales, etc.

Suelen ser aconsejadas tres medidas fundamentales para minimizar la vulnerabilidad con la particularidad de los activos de un SCI:

- Uso de 2 factores de autenticación, que si llevan password de un solo uso serían de máxima efectividad
- Uso de reconocimiento biométrico de usuario, que no solo mejora la seguridad, sino también la operatividad por las condiciones de trabajo del personal en los entornos industriales, especialmente en planta (ruido, fatiga, polvo, etc.) reduciendo errores.
- Uso de autenticación centralizada y si esto no es posible uso de *tokens* cifrados y firmados vinculados a una CA.

6.3.3. Vulnerabilidades y Actualización de Sistemas de Control Industrial SCI

La actualización de sistemas de control industrial puede conllevar efectos en procesos que afecten al funcionamiento del sistema conjunto, a su productividad, rentabilidad, etc. Si esto es algo evidente para IT, se duplica para OT en SCI donde hay mayor heterogeneidad de sistemas, activos, versiones, etc.

Los SCI no pueden replicarse en un entorno de pruebas para verificar una actualización previamente a su despliegue, lo que hace difícil el testeo del patching. Esa incertidumbre, sumada a que un SCI es un sistema de sistemas, conlleva a que los efectos no controlados sean de difícil evaluación en el sistema total, poniendo en peligro el funcionamiento y estabilidad global. Por todo lo anterior la colaboración con los proveedores de los distintos elementos HW y SW del SCI es fundamental para el despliegue de nuevas versiones de productos y sistemas o subsistemas.

La publicación de una actualización de un producto va asociada a una o varias vulnerabilidades que cada fabricante trata de manera distinta, a fin de evitar el impacto no solo tecnológico, sino también comercial, de imagen, etc. La gestión correcta de vulnerabilidades invita a compartirlas de forma pública mediante procesos lo mas abiertos posibles. Para ello existen organizaciones como CERT/CSIRT´s que tratan de ayudar en este sentido, siendo el de Estados Unidos uno de los mas importantes (Cyvbersecirity & Infrastructure Security Agency, 2022). En España disponemos del NCIBE-CERT. Es el centro de respuesta a incidentes de seguridad de referencia a nivel nacional. Esta gestionado por el Instituto Nacional de Ciberseguridad (INCIBE), que depende del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial

Una vulnerabilidad se publica con unos datos básicos:

- Fecha de descubrimiento y fecha de publicación
- Vulnerabilidades o avisos relacionados
- Sugerencias de riesgo asociado (CVSS, CVE/CWE, etc.)
- Resumen de riesgo e impacto
- Productos afectados
- Descripción técnica de la debilidad, vulnerabilidad y forma de explotación o prueba de concepto
- Soluciones propuestas para eliminar o mitigar el problema
- Etc.

Dichos datos después hay que interpretarlos y decidir si aplicar o no las soluciones propuestas. A tal fin se pueden seguir guías definidas por la organización o por entidades gubernamentales como las generadas por el Departamento de Seguridad Nacional estadounidense (Cibersecurity & Infrastucture Security Agency, 2022) que dan una idea de los pasos a seguir y criterios a aplicar, como por ejemplo

- Análisis de vulnerabilidades.- huella basada en cuatro elementos primarios con los que hacer una representación grafica: impacto, exposición, despliegue y simplicidad. Cuanto mayor es el tamaño de la huella mas vulnerable es el SCI y mas urgente es la mitigación del riesgo. Sea el siguiente ejemplo tomado del documento de referencia:

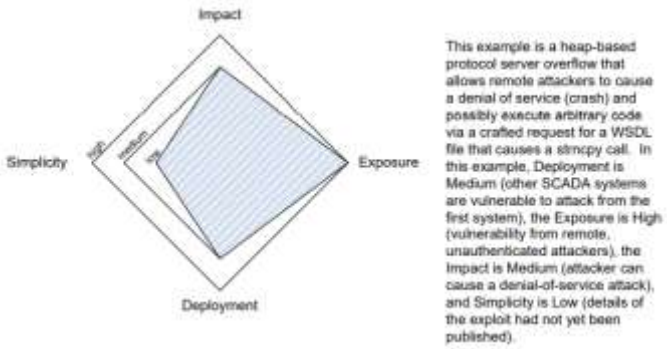


Figura 12 .- Ejemplo de huella de vulnerabilidad (Cibersecurity & Infrastucture Security Agency, 2022)

- Diagrama de flujo para la toma de decisiones.- proceso para determinar la urgencia de un parcheado en un SCI. Considera factores críticos para decidir qué hacer. El ejemplo de la referencia sería:

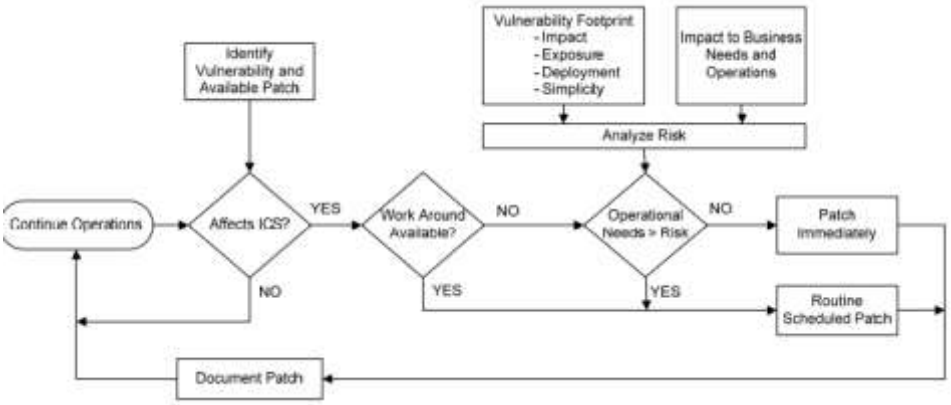


Figura 13 .- Árbol de decisión para decidir la urgencia de una actualización (parcheo) (CISA)

Las vulnerabilidades, como ya se ha insistido en varios puntos de este texto, se publican en organismos oficiales (National Computer Security Incident, 2022) y su consulta ayuda en esta toma de decisión, como pueden ser en EEUU:

- http://www.kb.cert.org/vuls/ (US-CERT vulnerability Notes Database)
- http://nvd.nist.gov/home.cfm (National Vulnerability Database USA)
- http://www.cert.org/other_sources/viruses.html (Software Engineering Institute and Carnegie Mellon for US-CERT.)
- etc.

O en Europa ENISA (European Union Agency for Cybersecurity, 2022).

Igualmente hay entidades de confianza para su consulta, conformadas por operadores y fabricantes que aportan labor de análisis e investigación de incidentes y que comparten entre ellos y con las entidades oficiales. Es el caso de *Information sharing and Analysis Centers (ISACs* (National Council of ISACs)) que se dividen por industrias o áreas de interés identificadas por ser un recurso clave para el funcionamiento de una nación o una sociedad por instituciones de

amplio reconocimiento a nivel internacional (*Critical Infrastucture Key Resource CIKR* (CISA, 2022)).

6.4. GOBERNANZA DE LA SEGURIDAD EN SCIs

6.4.1. Los sistemas operativos en un SCI

La variedad de sistemas operativos se dispara en los SCIs. Según la fuente consultada los datos son distintos. Las estaciones de trabajo suelen ser Windows, que pueden tener versiones antiguas e incluso posteriores a su EoL, aunque pueden tener Linux; los servidores pueden ser Unix y con versiones muy antiguas (SunOS) o modernas (Solaris, HP-UX) o bien Linux, con predominio de Red Hat Enterprise Linux, aunque con auge de Ubuntu y Centos; los terminales de trabajo de campo pueden ser móviles donde podría existir un MDM; y los dispositivos finales pueden tener RTOS que requieren de especial tratamiento.

Los sistemas operativos son muchos y su evolución muy variada, por lo que su control y parcheado resulta un reto en SCIs. Como muestra, las versiones de Linux disponibles y su evolución en el tiempo, que se pueden ver en (Wikimedia.ORG). Resulta conveniente disponer de soluciones centralizadas que gestionen las actualizaciones, aunque hay un gran abanico de posibilidades:

- Cada distribución de sistema operativo tiene soluciones de pago solo para esa distribución
- Soluciones *open source* como *Puppet*, *Chef* o *Ansible* con soporte comercial
- Soluciones comerciales combinadas para Microsoft y Linux y sus opciones varias.
- Etc.

Bastionar un sistema con un sistema operativo u otro requiere procedimientos, en base similares, pero en su desarrollo sustancialmente distintos. Así para un sistema Linux los pasos serían deshabilitar los servicios no utilizados, seguir las guías de seguridad de la distribución que sea, ejecutar *Lyns* (Lynis, an introduction) y gestionar el direccionamiento y filtrado de trafico de red (*host-based firewalls, iptables*, etc.) , intentar buscar soluciones de un tercer proveedor y automatizar las actualizaciones. Para otros sistemas operativos serán procesos, en lugar de servicios o demonios,

6.4.2. SIEMs y Protección de los elementos finales (EndPoints)

Como se ha venido haciendo a lo largo de todo el texto, y aunque las referencias son constantes y aparecen al final del documento, cada vez son mas las recomendaciones de uso de sistemas centralizados de gestión de incidentes e igualmente el despliegue de sistemas de protección en el elemento final.

La protección de los elementos finales se puede realizar de muchas maneras que se identifican por nombres como antivirus, control de aplicaciones en ejecución

(.exe con hash), control del entorno de ejecución (*sandboxing*), gestión de configuración e integridad de ficheros, contendores, *firewalls*, etc.

Esas protecciones, como funciones, las ofrecen unos productos si y otros no, de diferentes fabricantes, unos de pago y otros opensource pero sin contar con una solución universal tipo bala-de-plata.

Como características de esas posibilidades cabria señalar:

- Los antivirus son los mas conocidos y antiguos, y con ello los medios para evitarlos (Black hills, 2019).
- El control de aplicaciones en ejecución (ARC - *Application Runtime* Control) se basa en técnicas de listas blancas de aplicaciones identificadas por su firma o hash, que previene el malware que arranca con el sistema, aunque no evita otras técnicas como la inyección de código en proceso ya corriendo. Esta técnica es muy popular por su incorporación al ecosistema Microsoft mediante *AppLocker*.
- *Application Sandboxing*, considerado como un control de acceso obligatorio (MAC *Mandatory Access Control*), realiza un control de los programas a las interacciones del sistema operativo relativas a usuarios y servicios, ficheros, acceso a red, llamadas a sistema, acceso al registro, etc. Las herramientas mas populares para esta funcionalidad son SRP (*Software Restriction Policies*) y *AppLocker* en *Windows*; *SELinux* y *AppArmor* en Linux (Cybercity, 2009) y TrustedBSC en MAC OS.
- Control de integridad de configuraciones y ficheros durante el tiempo de vida del sistema que controla mediante *snapshot* el estado y lo compara para verificar modificaciones no autorizadas. Las herramientas opensource más utilizadas son *Tripwire* y OSSEC.
- Contenedores, que empezaron con comandos Unix que limitaban la ejecución de un proceso a un conjunto de ficheros y recursos y que con el paso del tiempo ha evolucionado tecnologías de contenedores y orquestadores para su control (*Docker*, *Kubernetes*, etc.) de manera que un proceso no solo se aísla del sistema total de ficheros, sino a recursos del *kernel*, de red, del árbol de procesos, de usuarios, etc.

No obstante, para detectar una intrusión o verificar que el sistema esta comprometido no hay mejor método que el análisis de logs, no siendo este el punto fuerte en las redes de los SCI, donde hay muchos elementos que no reportan todo lo que sería de esperar y consideran aquello que esta relacionado con el estado del arte de ciberseguridad por estar pensado con otra filosofía mas "industrial". Igualmente tampoco existe una conciencia de esta necesidad de su almacenamiento en el tiempo para generar una base de conocimiento y experiencia de cara al negocio y a la seguridad.

Las maquinas Windows, por ejemplo, parten de tres ficheros de log: de aplicación, de seguridad y de sistema; aunque disponen de otros (*Directory Service*, *File Replication Service*, etc.) y con ellos se puede analizar un fallo que se haya dado en un sistema. La definición correcta de una política de auditoria

permitirá el almacenamiento de logs con la información necesaria y el tiempo preciso para unas conclusiones determinantes.

El siguiente paso es el almacenamiento centralizado de logs de manera que se prevenga la manipulación o corrupción de logs en las maquinas origen y se pueda mejorar el análisis general del SCI, correlando y analizando todo de forma uniforme en la organización. De esa idea surge el SIEM – Security Information and Event Management – (*Spliunk*, IBM *QRadar*, *LogRhythm, Elastic Stack – Elastick* Search, *LogStash* y *Kibana*-). Se produce una variación de los protocolos de generación, almacenamiento y tratamiento de logs para ser remitidos desde cada elemento con un agente a un sitio determinado (o mediante colectores en una jerarquía de adquisición de eventos y logs) donde no solo se almacena la información sino que se produce una correlación en tiempo real y generación de alamas generales y provisión de un interfaz de análisis para el tratamiento de amenazas, incidentes de seguridad y análisis forense.

Para entornos industriales la recolección sería tal y como muestra la figura:

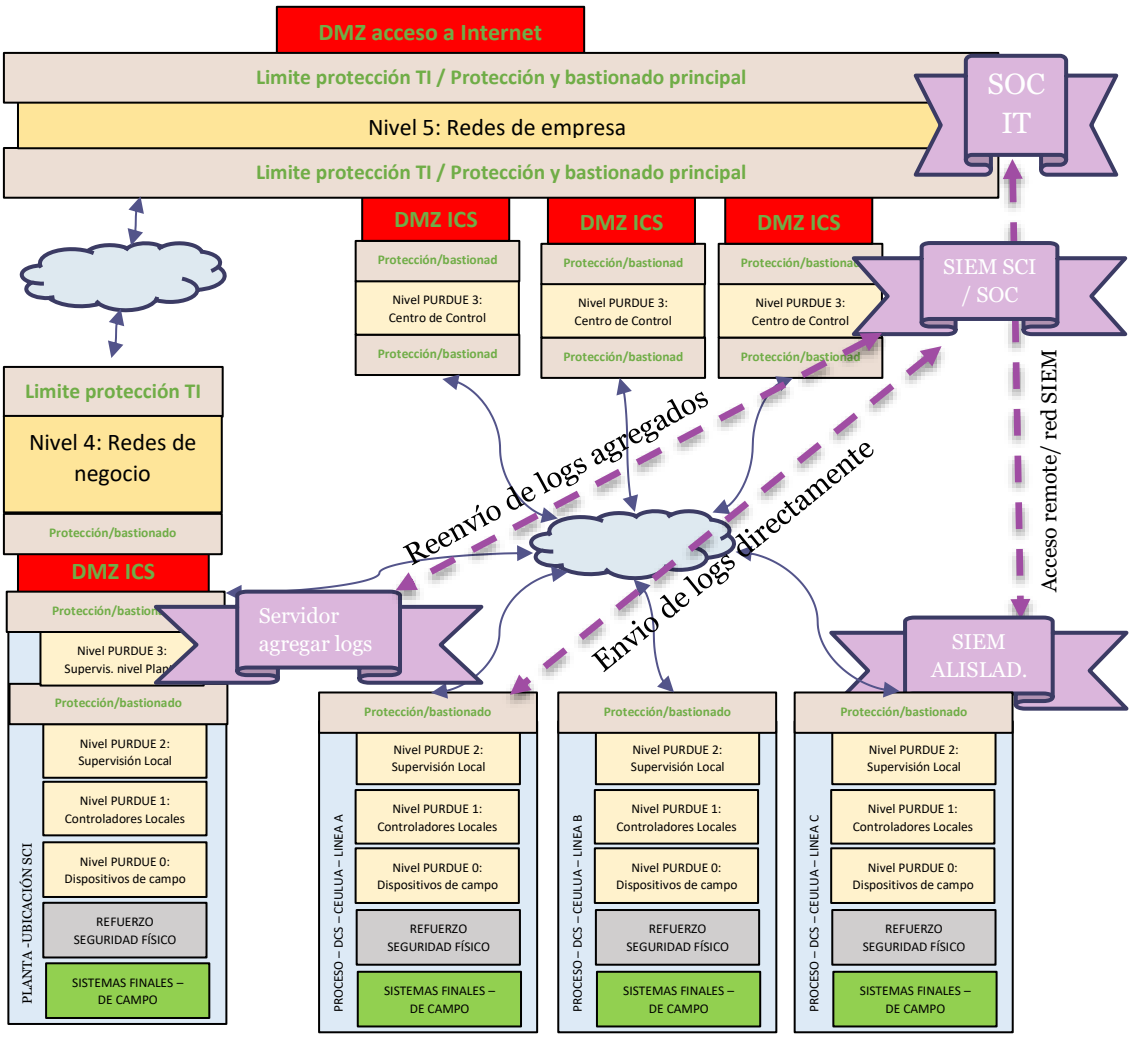


Figura 14 .- Jerarquía logs y SIEMs en SCI

La recolección de logs debería ser de forma centralizada y a ser posible desde un lugar fuera de la red de control, de forma aislada. Esto permitiría a los ingenieros de control acceder a los datos que necesiten, pero que el personal que se dedique a la seguridad disponga de la información sin interferir en los procesos, aunque con las medidas de seguridad adecuadas dentro de esa otra red que hará falta que se interconecte a la de negocio.

A partir de la información disponible se debe perfilar la actividad normal de la que no lo es para detectar cualquier anomalía que pudiera estar asociada a un ataque al sistema.

6.4.3. Cultura de Ciberseguridad para SCIs.

La cultura de la ciberseguridad empieza por las políticas y programas de seguridad deben ser establecidos en las organizaciones implicando el mayor número de estamentos y personas posibles, aunque solo en el ámbito que le corresponda a cada entidad. Los pasos serían:

1. Obtener el apoyo de la dirección.
2. Crear un equipo con las aptitudes adecuadas dedicado a la seguridad.
3. Identificar los requisitos de la organización (de negocio, normativos, etc.) y los riesgos existentes.
4. Establecer una política de seguridad y los procedimientos que la desarrollan.
5. Llevar a efecto lo planificado con principios de mejora continua y carácter circular.

La seguridad no se establece de forma mágica con un producto único. Las soluciones se establecen por niveles y por sistemas, orientándose a una defensa en profundidad con todo lo necesario: prevención, detección y respuesta

Figura 15.- Ejemplo de defensa en profundidad.

Existen tres marcos de referencia que dan un método organizado para implantar un programa de seguridad:

- ISA/IEC 62443 (Internationl Society of Automation, 2022),
- ISO 27001 (ISO/IEC 27001 Information Security Management) y
- NIST CSF (NIST Cybersecurity Framework, 2022).

Las funciones principales de las arquitecturas vienen a ser las mismas. Pongamos las del NIST CSF que es el único documento gratuito:

- **Identificación,** da como resultado las bases para la estructura pues señala y define el contexto de negocio, los recursos vinculados a funciones críticos y los riesgos ciber asociados. De esos resultados sale la dirección a tomar en las acciones.
- **Protección,** generando las salvaguardas que aseguren el servicio o proceso que contienen un posible evento de seguridad
- **Detección,** procurando lo necesario para detectar un evento de ciberseguridad, manejando los términos de anomalías y eventos, monitorización continua, etc.
- **Respuesta,** adaptando los medios de la organización a un posible incidente para minimizar su impacto.
- **Recuperación,** de cara a mantener capacidades y servicios ofreciendo resiliencia y restablecimiento de aquello necesario.

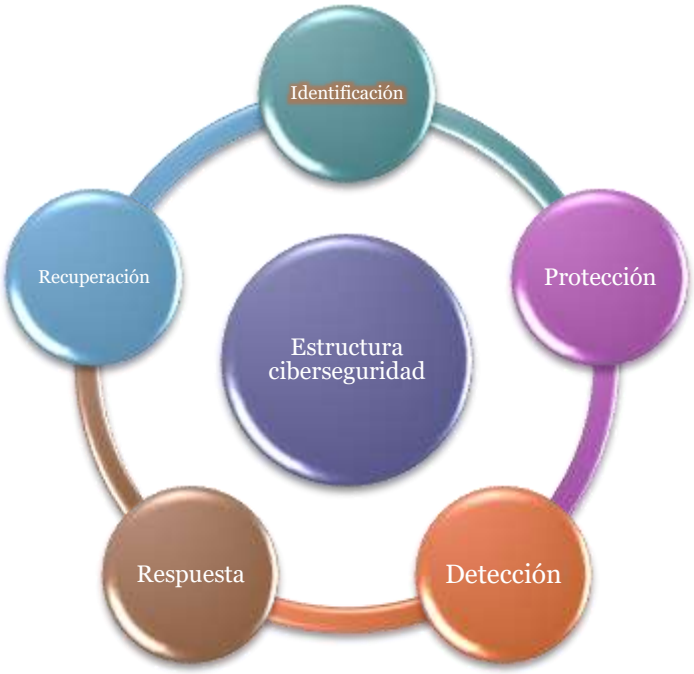


Figura 16 .- Principios o funciones principales de una estructura de ciberseguridad

En dichos marcos de referencia se ofrecen los distintos niveles que marcarían como una organización ve el riesgo en ciberseguridad y como lo trata, o mas bien como esta el marco de implantado en la organización.

	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

Figura 17 .- Niveles de implantación del marco de referencia NIST. Versión 1.1

6.4.4. Estructura documental de Ciberseguridad para SCIs.

La ciberseguridad en una organización mediante un programa incluye varios tipos de documentos en los que el matiz esta en gran medida, aunque no únicamente, en la obligatoriedad de su cumplimiento, en el nivel de detalle en que se establecen objetivos, etc.

Con carácter general se establecen (o no) y se tienen (o no):

- Políticas, con los objetivos globales que se expresen de forma clara y concisa y se ajusten a criterio SMART (*Specific*, *Measurable*, *Achievable*, *Realistic, Time-based*) y que identifiquen quién, qué, donde, cuándo y por qué. Resulta imprescindible contemplar la cultura de cumplimiento en toda la organización y los mecanismos de control de cumplimiento que permitan la correcta valoración.
- Normas , con los requisitos generales, donde se establece lo que debe o no hacer y es exigido conforme a la norma hecho se fijan los términos relativos en la norma RFC 2119 (IETF.ORG)
- Guías, con las recomendaciones, donde se indica lo que debería ser o no conforme a la misma norma.
- Procedimientos, con los pasos a seguir para lograr un objetivo. Se incluyen requisitos de las normas, a ser posible con las recomendaciones de las guías, etc.

El seguimiento de la norma ISO27001 permite definir los documentos para un programa de ciberseguridad, con un listado de políticas y procedimientos a partir de los que se puede crecer. De hecho, dependiendo del ámbito geográfico, político, de actividad o económico, un sistema puede tener restricciones normativas si no se siguen estas normas y recomendaciones.

Así por ejemplo la corporación NERC establece las normas necesarias para considerar seguro un entorno dentro de Estados Unidos. En la referencia (North American electric Reliability Corporation) disponemos del listado de normativa aplicable:

Mandatory Standards Subject to Enforcement

Standard Number	Title	Contains Retired Requirements	Related Information
(BAL) Resource and Demand Balancing (10)			
(CIP) Critical Infrastructure Protection (12)			
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization		Related Information
CIP-003-8	Cyber Security — Security Management Controls		
CIP-004-6	Cyber Security - Personnel & Training		Related Information
CIP-005-6	Cyber Security — Electronic Security Perimeter(s)		Related Information
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems		Related Information
CIP-007-6	Cyber Security - System Security Management		Related Information
CIP-008-6	Cyber Security — Incident Reporting and Response Planning		
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems		Related Information
CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments		Related Information
CIP-011-2	Cyber Security - Information Protection		Related Information
CIP-013-1	Cyber Security - Supply Chain Risk Management		Related Information
CIP-014-2	Physical Security		Related Information

Figura 18 .- Normativa aplicable

6.4.5. Medidas de Ciber-Riesgo en una organización

Para medir los riesgos a los que una organización esta expuesta se pueden usar métodos

- cuantitativos, dando a cada riesgo un valor numérico
- o cualitativo, donde se dan rangos de riesgo según sea bajo-medio-alto o con una nota de 1 a 10.

Para categorizar el riesgo es conveniente entenderlo lo mejor posible: qué compromete o podría comprometer ese riesgo en la organización, que tipo de amenaza es, que vulnerabilidad se explota, qué efecto se produce para la organización y cómo impacta, qué probabilidad de que ocurra tiene, con qué frecuencia, cómo es de difícil explotar la vulnerabilidad, etc.

Calculado el riesgo, independientemente del método usado, la persona autorizada en la organización establece cómo tratarlo (aceptarlo/combatirlo). Normalmente se consideran los costes de las contramedidas necesarias para contrarrestar un riesgo con los efectos del mismo. Cabe señalar como contramedidas especialmente beneficiosas que protegen el retorno de la inversión los planes de:

- *Disaster Recovery*: orientadas a recuperar los sistemas y procesos que se puedan ver afectados
- *Bussines Continuity*: pensando en las acciones que garanticen la estabilidad del servicio o razón de ser de la organización.

Estos dos planes incluyen ciertos pasos que se consideran necesarios, como son el inicio del proyecto, su evaluación, el análisis de riesgos y su impacto, la creación

de un plan de recuperación ante desastres o continuidad de negocio, su evaluación y terminar el ciclo de mejora continua con la actualización y aprobación del nuevo proyecto de plan que da inicio a otro recorrido completo:

Figura 19 .- Ciclo planes de recuperación y de negocio

6.4.6. Respuesta a incidentes.

Dada la importancia de los incidentes en los SCI, es importante fijar un protocolo de actuación o respuesta ante ellos. Esto se hace en base a una evaluación correcta y consensuada dentro de la organización de los riesgos. Una posible referencia para esto es la dada por Departamento de Energía de los EEUU (DOE) que estableció un proceso de 6 pasos que después fue adaptado por la norma NIST 800-61 (NIST - Computer Security Resource Center):

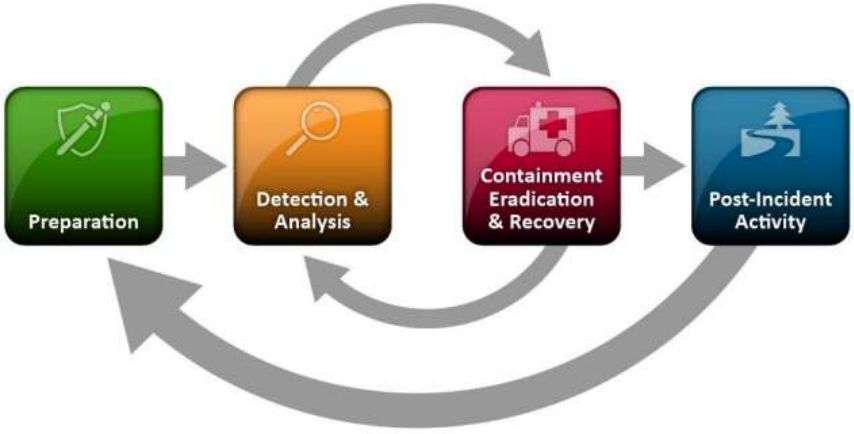


Figura 20 .- Proceso de Plan de Respuesta a Incidentes NIST

- **Preparación**, que debe hacerse con antelación al incidente, dotando al sistema (recursos físicos y materiales) de los medios necesarios para tratar un incidente y que van desde una sala de reuniones adecuada a un listado de a quien llamar según para qué.
- **Detección y Análisis**, identificando primero qué es un incidente para la organización y de que clase o categoría. Es importante separar incidentes de eventos y mucho más de "posibles eventos". Asimismo conviene tener sistemas de correlación de información (IDS, actividad de red o de usuario anormal, incidencias en procesos SCI, etc.) para poder dar una alerta temprana, sin precipitar las conclusiones. Por último en este punto hay que asignar el encargado de la incidencia y la cadena de acciones para tratar o escalar el tratamiento.
- **Contención**, para minimizar el impacto y estabilizar el entorno mediante el aislamiento si se puede sin empeorar la situación. Una vez contenida la situación se deben obtener evidencias de lo ocurrido e identificar la fuente del incidente, actualizando los indicadores de compromiso (IoC).
- **Erradicación**, para eliminar tanto el malware como los puntos de entrada a la organización antes de restaurar los sistemas para no exponer de la misma forma el sistema.
- **Recuperación**, asegurando que no se restaura aquello que estaba afectado, y eso o bien instalando todo desde el principio de forma segura o restaurando el sistema de una copia de seguridad de un estado en el que se puede confiar. Además de eso pasar a producción requerirá un proceso de pruebas y la autorización del personal con esa capacidad en la organización.
- **Actividad post-incidente**, para sacar las conclusiones mas relevantes y puntos de mejora de manera consensuada entre todos los participantes para trasladar el mensaje adaptado a toda la organización, si fuese necesario, y generar un conglomerado de lecciones aprendidas.

6.5. Arquitecturas IoT e integración con SCI

6.5.1. Introducción

IoT esta revolucionando multitud de áreas de nuestra vida diaria y el mundo de los negocios, tanto en la forma de interactuar con el entorno como en la manera de afrontar el futuro. Multitud de trabajos y tecnologías se enfrentan a recoger información en forma de pequeños datos desde el rincón más recóndito de cualquier sistema, pero el reto está surgiendo en la visión holística de IoT, una parte más de la transformación digital de nuestro modo de vida.

IoT ha pasado ya su fase inicial de dispositivos inmaduros con tecnologías emergentes de captación de datos. Los dispositivos finales son cada vez más fiables. Asimismo las técnicas de machine *learning*, tecnologías de *cloud* o edge computing y blockchain hacen de IoT un paradigma en creciente expansión y desarrollo donde no solo se genera información, sino que se integra en un mundo

colaborativo, heterogéneo y capaz de predecir las necesidades de personas y sistemas.

Estudios llevados a efectos por grupos como *Gartner* o BCG marcan las principales tendencias basadas en IoT y en la generación de conocimiento basada en diversas tecnologías a partir de los datos sensados por millones de dispositivos en cualquier sitio, momento y de cualquier magnitud.

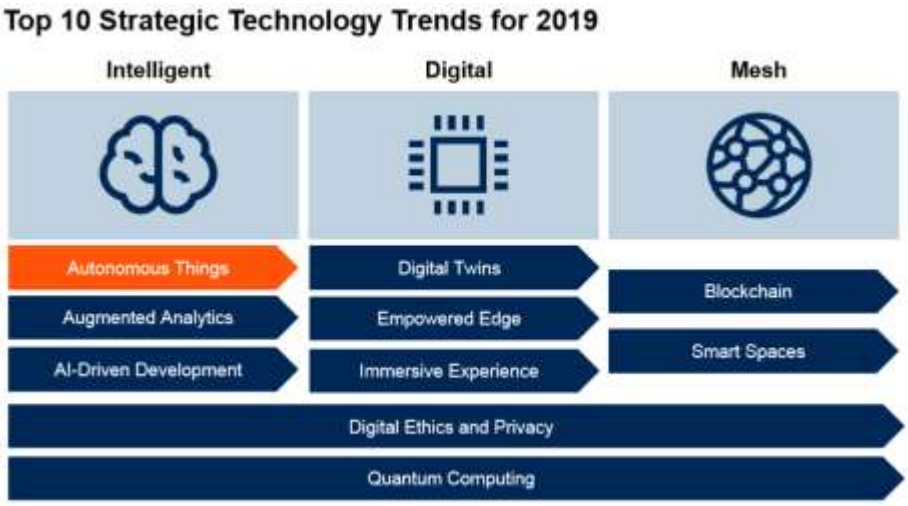


Figura 21 .- Tendencias tecnológicas según Gartner

Las aplicaciones se han disparado y el dato empieza a ser el objetivo principal. El mantenimiento predictivo en procesos industriales sigue en auge, aunque ha perdido fuerza y es en otras áreas donde surge la posibilidad de aplicación. Así, por ejemplo se consigue a través de los datos proporcionados por sus cámaras y sistemas de seguridad proporcionar orientación en cuanto a demografía y comportamiento de los clientes de los negocios a los que dan protección.

El uso de inteligencia artificial, machine *learning*, realidad aumentada y virtual y blockchain favorece la oportunidad de negocio de IoT en entornos donde ya se proyectaba su impacto: automoción, sanidad, logística, etc. traspasando las de lo industrial o comercial a lo personal, de lo artificial a lo natural, de lo profesional a lo lúdico….

La exposición del estado del arte de los distintos puntos tecnológicos irá de mas a menos nivel de concreción, yendo desde las arquitecturas generales de las tecnologías y los casos de uso a una descripción del paradigma en torno al cual giran estas arquitecturas (sería IoT) y un punto concreto de este entorno que va a ser la piedra angular del desarrollo del TFM, que seria el “edge computing”

6.5.2. El concepto de arquitectura para IoT

El concepto de arquitectura surge a partir de una serie de requerimientos de los sistemas que incorporan IoT, y más en el entorno industrial (IIoT):

- Conectividad y comunicación
- Gestión y control de dispositivos

- Recabar, analizar y actuar datos o sobre los datos
- Escalabilidad, Integración y Flexibilidad
- Alta disponibilidad
- Seguridad

La implementación de un sistema que se adapte a estos requerimientos se hace a partir de una división principal en niveles que agrupan tanto las tecnologías como los servicios: dispositivos, enrutamiento de la información, red, nube, aplicación, seguridad, gestión, etc. La granularidad puede ser mayor o menor en función del sistema o del proveedor, pero una estructura que parece estar adoptándose es la arquitectura que ha adoptado Microsoft. Se resume en tres niveles de trabajo: a nivel de dispositivo y del dato sensado, a nivel de conocimiento basado en los datos, a nivel de acciones derivadas de dicho conocimiento. Es una idea común a todas, y ésta es la de dividir en tres partes que son:

- dispositivos,
  - incorporar dispositivos
  - actualizarlos
  - configurarlos conforme a la aplicación
  - operativa remota
- edge (cada vez más inteligente), o conectividad y comunicación
  - dispositivos – *hubs/gateways*
  - hubs/gateways – nube
  - protocolos basados en eventos, subscripción, mensajes, etc.
- *cloud* o analítica y aplicaciones
  - generación de valor
  - visualización
  - acciones y decisiones

De esta manera, cualquier arquitectura, por funcionalidades que tenga se puede dirigir a tres niveles aunque los niveles de edge y cloud cada vez se limitan por líneas más desdibujadas debido a la mejora de los dispositivos y las comunicaciones, cada vez más potentes en su capacidad de proceso, cálculo y tratamiento de información.

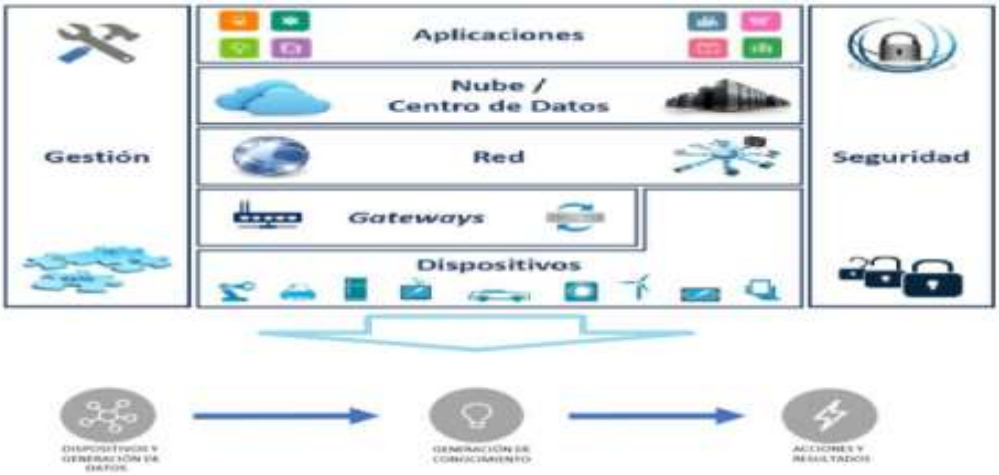


Figura 22 .- Arquitectura IoT. Modelo general

Este modelo general de la arquitectura IoT va desglosándose en capas y subsistemas, y además se da lugar a una matriz con las funcionalidades mencionadas más arriba. Los subsistemas principales serían:

- Dispositivos.- incluyendo los hubs y gateways de extremo que tienen la capacidad de interconectarse a elementos concentradores de mayor jerarquía y capacidad antes de elevar la información a la nube de forma segura. Tratan los datos en bruto o una vez pre-procesados, si incluyen esas capacidad ("*intelligent edge devices*"),
- Sistema concentrador de nube.- o llamado en algunos entornos "de agregación", que se encarga de recibir vía un *hub* o *gateway* los datos enviados por sus colaterales de extremo (edge), con gestión de dispositivos y adquisición de datos. Es la capa real de intelligent edge devices, y se dispondrá de infraestructura necesaria para el registro y conexión de los dispositivos con la escalabilidad suficiente para adaptarse a un sistema donde la gran cantidad de dispositivos e información es una característica esencial. Otras opciones son las dedicadas al pre filtrado y pre procesado de datos "*data transformation*".
- Sistemas de procesado.- tanto de procesado de grandes cantidades de datos como de síntesis de información para procesos de negocio y su almacenamiento. El procesado de grandes ráfagas de datos y sus reglas de comportamiento serán un factor determinante para caracterizar estos sistemas
- Sistemas de visualización y gestión de elementos.- para operadores y usuarios en general, que permitan integración con *CRMs*, envío de notificaciones y alarmas, etc. Se puede disponer de funcionalidades añadidas como "machine learning" y "*user management*"
- Sistemas de almacenamiento.- que incluyen datos que deben estar disponibles para reporte y visualización inmediata y datos almacenados a largo plazo para su procesado posterior.

Esta idea, en línea con lo indicado más arriba, ha sido la adquirida por Microsoft y se está convirtiendo en una norma de facto que permite desarrollar fácilmente ecosistemas IoT.

Esta arquitectura es fácilmente relacionable con la establecida para SCI, estableciendo una relación uno a uno fundamentalmente con los niveles 0 a 3 de Purdue.

6.5.3. Arquitecturas de referencia concretas

Actualmente hay muchas tendencias y grupos trabajando en estándares IoT que van enfocadas a la integración de las nuevas tecnologías y fórmulas de trabajo que permiten una mejor interoperabilidad, eficiencia y eficacia en el manejo de datos e información.

Algunas arquitecturas de referencia IoT son

- Norma ISO/IEC 30141 sobre Internet de las Cosas (IoT) – Arquitectura de Referencia, el cual va a proporcionar un marco de referencia para los diseñadores y desarrolladores de aplicaciones IoT. (ISO-IEC International Organization for Standarization, s.f.)
- Arquitectura de referencia de Internet Industrial (IIRA), a partir del consorcio en marzo de 2014 de AT&T, Cisco, General Electric, IBM e Intel, orientados a aplicaciones de IoT industriales (Industry IoT Consortium, 2019)
- Internet of Things – Architecture (IoT-A) .- Generado en 2013 por un grupo de trabajo de la UE (Interrnet of Things Architecture, 2022)
- IEEE P2413 Estándar para una Infraestructura Arquitectónica para el Internet de las Cosas (IoT) generada por el IEEE conforme a la norma internacional ISO/IEC/IEEE 42010:2011

Veremos una arquitectura normativa (ISO), una arquitectura IoT aplicada al ámbito industrial (IIRA) y por último un modelo comercial (Microsoft) (www.microsoft.com, 2022)

6.5.3.1. Arquitectura de Referencia IoT normativa. ISO/IEC 30141

Dentro de la arquitectura normativa según ISO/IEC resulta complicado dar una idea en una imagen. En la Norma ISO/IEC 30141 se define una arquitectura de referencia (IoT RA) en base a un modelo conceptual (CM basado en las características de un sistema IoT, sus elementos y lo esperado en su total), un modelo de referencia (RM) con arquitecturas diferentes puntos de vista (visión funcional, de sistema, de comunicaciones, de información y de uso).

El modelo conceptual incluye los conceptos IoT clave y sus relaciones. Tenemos dominios que incluyen entidades, donde una entidad puede ser una o varias entidades digitales, físicas, un usuario IoT o una red.

Dentro de cada entidad se pueden encontrar conceptos particulares y la descripción de su funcionalidad y manera de integrarse en el modelo. Así por ejemplo se definen los conceptos de *endpoint*, componente o dispositivo IoT; conceptos como almacén de datos, red o Gateway IoT; y servicio y aplicación y cómo interaccionan todos.

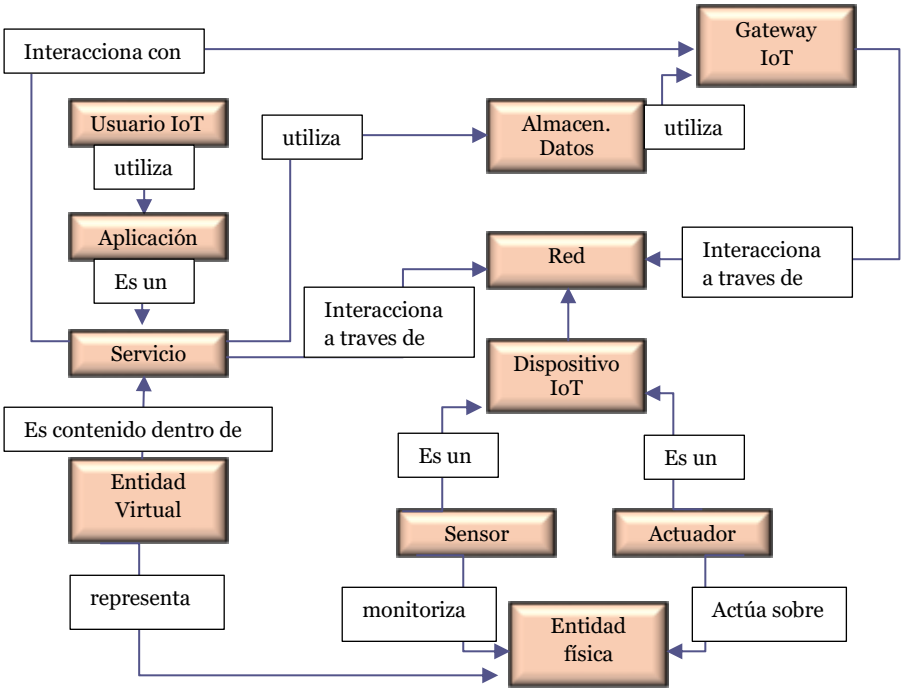


Figura 23 .- Ecosistema IoT

Y con estos conceptos, entidades, etc. surge una propuesta de arquitectura que vendría a sintetizarse en la siguiente figura:

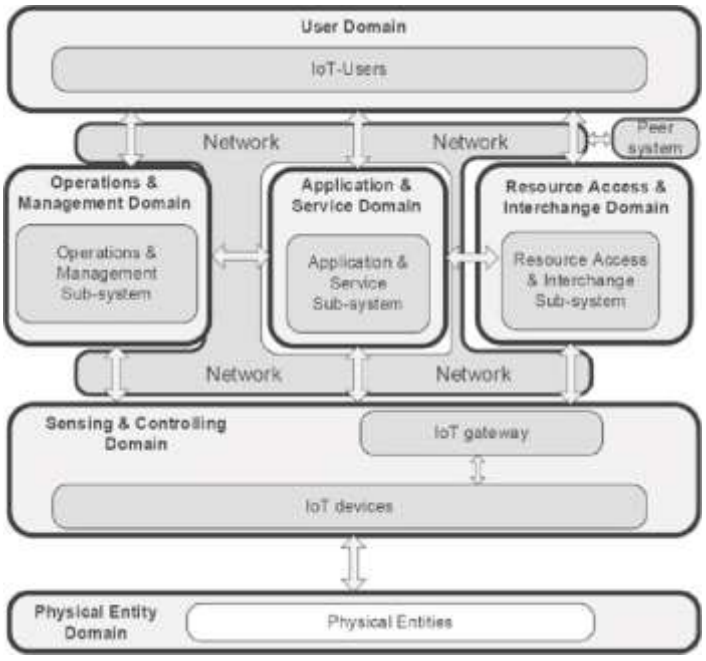


Figura 24 .- Arquitectura IoT. Propuesta

6.5.3.2. Arquitectura de Referencia IoT aplicada. IIRA

Esta Arquitectura de Referencia de Internet Industrial (IIRA) esta orientada a sistemas de Internet Industrial de las Cosas (IIoT). Especifica un Marco de

Arquitectura industrial de Internet (IIAF) que engloba todo lo necesario para definir IIRA (vocabulario, puntos de vista, etc.). Es una interpretación de la arquitectura de IoT definiendo conceptos apoyándose en la norma ISO 'ISO/IEC/IEEE 42010:2011. El objetivo es conseguir la máxima interoperabilidad entre fabricantes y productos para favorecer el desarrollo de tecnologías.

Se definen los conceptos necesarios, así como un marco de la arquitectura y los putos de vista para su estructuración: negocio, uso, funcional y de implementación. IIRA agrupa los elementos de la norma ISO para generar sus propias arquitecturas, sin desviarse de las normativas.

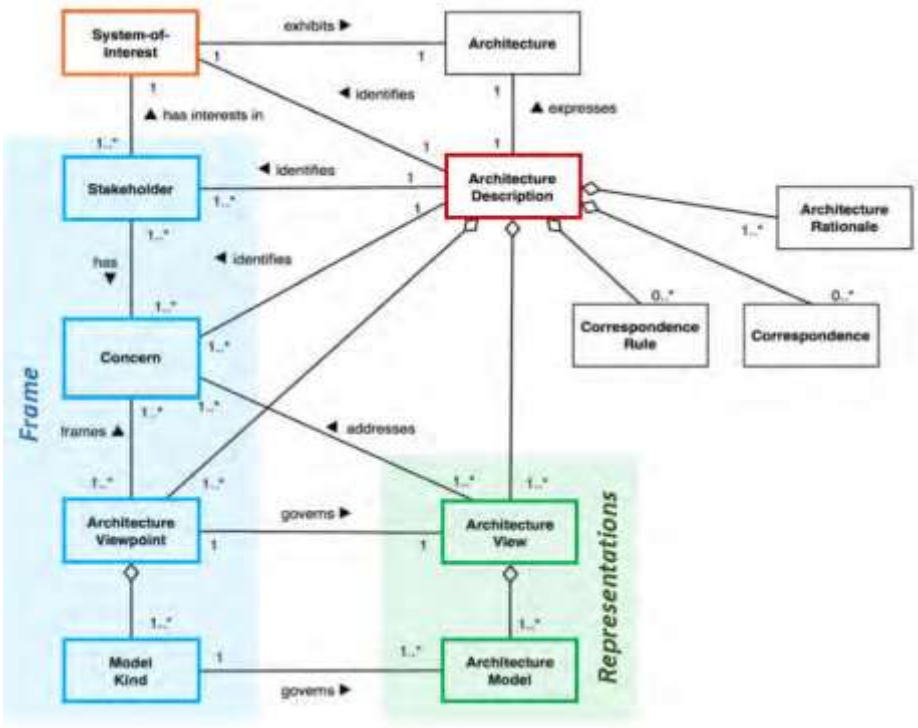


Figura 25 .- Arquitecturas IIRA vs ISO42010

El IIAF adopta los conceptos generales ISO. Se definen dos elementos:

- El marco de la arquitectura, que se define con: motivación, *stakeholders* y punto de vista.
- una representación de la arquitectura que se lleva a efecto con dos elementos: vistas y modelos.

Lo primero se identifica la razón de ser de IoT en el ámbito industrial para darle después una visión que englobe a todos los *stakeholders* y dando en definitiva una representación abstracta de esa arquitectura. No se entra en sistemas concretos ni reglas de construcción especificas, simplemente se adopta la especificación de la arquitectura conforme a la ISO 42010 de forma conceptual.

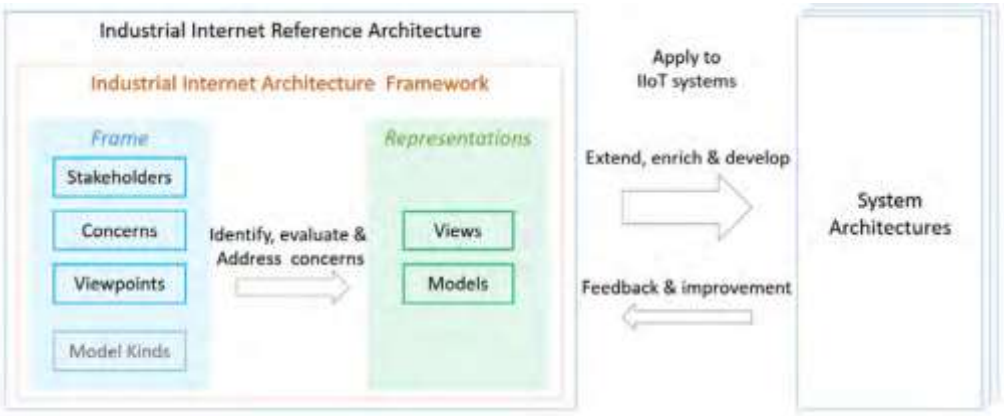


Figura 26 .- Estructura conceptual arquitectura IIRA

Lo primero que se establecen son los puntos de vista (*viewpoints*) analizando los casos de uso (identificados por el IIC) que sean aplicables, identificando los *stakeholders* de los sistemas IIoT y aquello que sea de interés con esos elementos. Hay cuatro *viewpoints*:

- de negocio, donde se traza la visión, valores y objetivos de los *stakeholders* del negocio para introducir IIoT en sus organizaciones. Los conceptos que se manejan son tales como retorno de inversión, capacidades fundamentales, etc.
- uso, donde se plasma como se alcanzan las capacidades clave mediante un sistema IIoT. Se manejan los términos de actividad (mediante la cual se usa el sistema), tarea, rol, mapa funcional de componentes, mapa de implementación, etc.
- Funcional, donde se estructuran las capacidades funcionales, a partir de las funciones clave, y la estructura del sistema. Se desglosan las funcionalidades por dominios:
  - Dominio de Control
  - De operaciones
  - De Información
  - De aplicación
  - De negocio
- y de implementación, donde se lleva a cabo una representación técnica del sistema. Los conceptos que se manejan son dispositivo, interfaz, protocolo, conexión, interconexión

Esos cuatro *view points* son muy abstractos y han de integrarse en el sistema, pero no solo en el diseño, sino en la totalidad del ciclo de vida del mismo, que varía de la industria de la que se trate e incluso del desarrollo concreto:

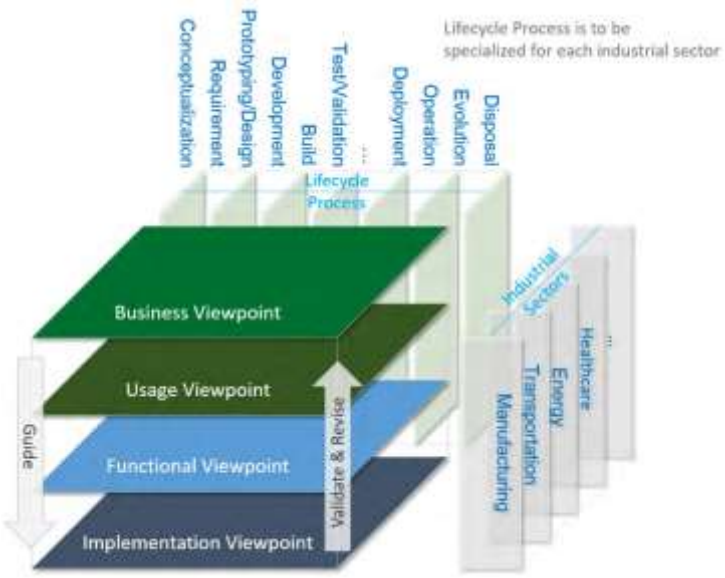


Figura 27 .- Relación *viewpoints* IIRA, aplicación y ciclo de vida del Sistema

Se proponen tres modelos-ejemplo de arquitectura, que se muestran mediante figuras para mostrar una idea de su fin, aunque esta fuera del propósito de este texto su detalle. No obstante, resulta necesario para después razonar su uso:

- Modelo de arquitectura de tres niveles conforme a una vision

Figura 28 .- Arquitectura a tres niveles IIRA visión A

o a otra visión

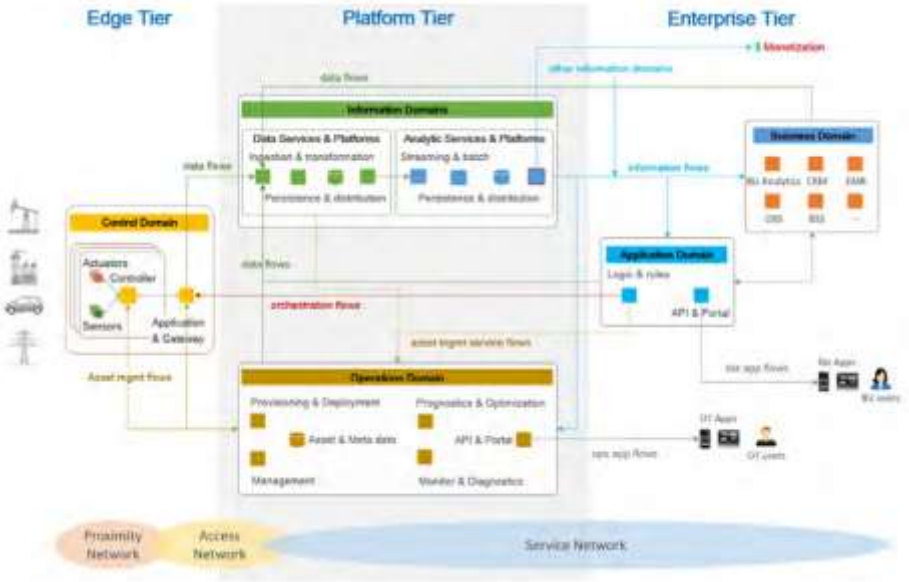


Figura 29 .- Arquitectura a tres niveles IIRA visión B

- Modelo de arquitectura de gestión y conectividad con el extremo mediante Gateway

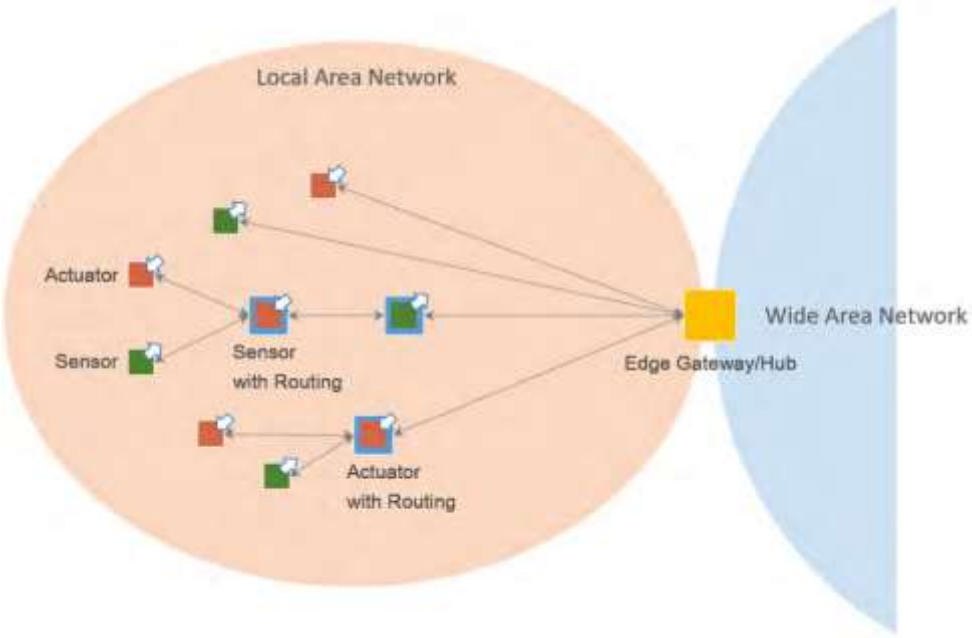


Figura 30 .- Arquitectura IIRA con conexión a edge por Gateway

- Modelo de bus de datos por niveles, que caso de ser tres niveles se muestra como en la siguiente figura:

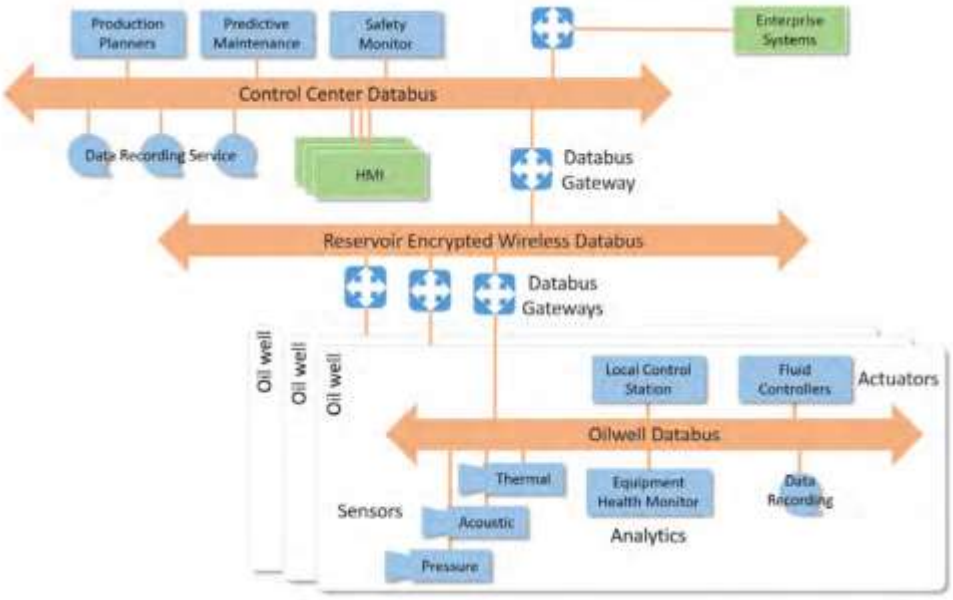


Figura 31 .- Arquitectura con bus de datos por niveles IIRA

6.5.3.3. Arquitectura de Referencia Microsoft

Por ultimo se presenta de forma somera para no acometer la enumeración de productos comerciales detallada de la arquitectura propuesta por Microsoft. Se presenta una arquitectura recomendada para aplicaciones de IoT que utilizan componentes *Azure PaaS* (plataforma como servicio). En el diagrama siguiente se reflejan diferentes componentes de *Azure* que se pueden usar para diseñar una solución de IoT. Se muestran todos los servicios disponibles, aunque en cada sistema o implementación se pueden usar solo los necesarios:

Figura 32 .- Arquitectura solución Microsoft para IIoT

La solución Microsoft, que pasa por *Azure* como *Paas* de este proveedor ofrece soluciones para entornos industriales como:

- Procesamiento de datos de un vehículo

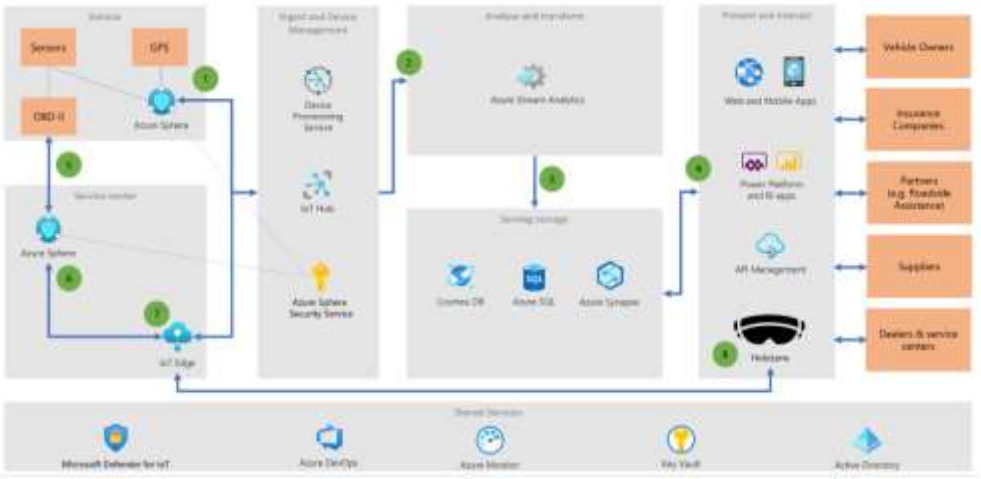


Figura 33 .- Arquitectura Microsoft IIoT. Caso de uso 1

- Supervisión del estado de IoT industrial

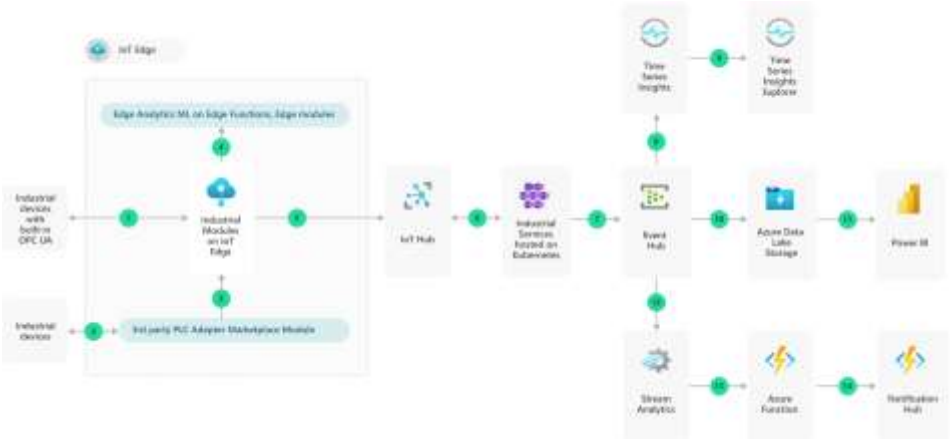


Figura 34 .- Arquitectura Microsoft IIoT. Caso de uso 2

7. Análisis del problema

Una vez finalizado el estudio sobre el estado del arte se debe establecer el análisis del problema al que este trabajo se enfrenta, identificando el objetivo que se persigue con los pasos que se estiman necesarios.

El objetivo es:

> "Definir una arquitectura segura de un sistema de control industrial que incluya IoT conforme a normativa nacional de manera que se garantice su integración en la infraestructura TI de la organización."

La arquitectura debe incluir los elementos recomendados por la entidad estatal de referencia de cara a una posible acreditación por su parte.

De manera más concreta, y una vez que se haya especificado la arquitectura general se hará una aproximación sobre un caso de uso. Se tomará un sistema de control industrial en un entorno que podría ser una infraestructura crítica, como es una terminal aeroportuaria.

Figura 35.- Caso de Uso .Aeropuerto de Valencia. Terminal de carga. Clasificación equipaje

Se integrarán en todo lo posible términos cercanos al uso final del sistema, apoyándonos en:

- Definición de servicio y Terminología de transporte intermodal (Ministerio de transporte, movilidad y agenda urbana, s.f.)
- Integración en una terminal de carga aérea real, como es la de Valencia (AENA, s.f.)

7.1. Especificación de Requisitos

Utilizando como guía la especificación de requisitos de *Volere* (Volere, s.f.), podrían definirse los siguientes aspectos:

- Requisitos funcionales
- Requisitos no funcionales
- Ajustes al entorno tecnológico y de negocio
- Motivaciones específicas

7.1.1. Requisitos Funcionales

Id. Requisito	RF1	Tipo de Requisito		Id. Caso de uso	
Descripción	Se especificarán los distintos niveles que puede tener una arquitectura que se ajuste al modelo				
Razón fundamental	Se determinan cuantos niveles son necesarios y cuantos posibles de manera que se solventen las distintas casuísticas alcanzables				
Criterio de valoración	Definición de niveles de 0 a 5 conforme PURDUE ajustado a normativa aplicable y criterios de autoridad certificadora				

Id. Requisito	RF2	Tipo de Requisito		Id. Caso de uso	
Descripción	Se especificarán los distintos elementos que en los distintos niveles puede tener una arquitectura que se ajuste al modelo.				
Razón fundamental	Se determinan funcionalmente que equipos son necesarios y cuales posibles de manera que se solventen las distintas casuísticas alcanzables				
Criterio de valoración	Definición de elementos IT-OT-IoT encajables en la arquitectura conforme a las definiciones establecidas				

Id. Requisito	RF3	Tipo de Requisito		Id. Caso de uso	
Descripción	Se especificarán los distintos DMZs que separarán los distintos niveles que puede tener una arquitectura que se ajuste al modelo.				
Razón fundamental	Se determinan funcionalmente que DMZs son necesarios y cuales posibles de manera que se solventen las distintas casuísticas alcanzables				
Criterio de valoración	Definición de DMZ entre cada nivel o grupo de niveles y características del equipamiento y la funcionalidad del mismo				

Id. Requisito	RF4	Tipo de Requisito		Id. Caso de uso	
Descripción	Se especificarán que sistemas compondrán cada nivel y con qué herramientas se puede hacer en un ejemplo practico				
Razón fundamental	Conseguir especificar un caso de uso en su totalidad.				

7.1.2. Requisitos No Funcionales

Id. Requisito	RNF1	Tipo de Requisito		Id. Caso de uso	
Descripción	Definir arquitectura base ajustada a la norma IEC62443				
Razón fundamental	Uso de una norma y criterio de ámbito internacional y procedente de una organización de referencia sin animo de lucro.				
Criterio de valoración	Uso de criterios de norma: definición de niveles y espacios en la infraestructura propuesta				
Documentación	(IEC WebStore International Electrotechnical commisssion, s.f.)				

Id. Requisito	RNF2	Tipo de Requisito		Id. Caso de uso	
Descripción	Seguimiento guías y recomendaciones de INCIBE.				

Razón fundamental	Uso de referencias que permitan la acreditación de sistemas por entidades autorizadas en el ámbito nacional e internacional.
Criterio de valoración	Uso de mismos elementos y criterios que las guías y recomendaciones
Documentación	(INCIBE-CERT, 2022)

Id. Requisito	RNF3	Tipo de Requisito		Id. Caso de uso	
Descripción	Realizar otras propuestas a partir de la arquitectura base que introduzcan tecnologías IDS/IPS y SIEM				
Razón fundamental	Garantizar la seguridad de la arquitectura propuesta conforme a parámetros de autoridad nacional				
Documentación	(INCIBE)				

7.1.3. Ajustes al entorno tecnológico y de negocio.

Id. Requisito		Tipo de Requisito		Id. Caso de uso	
Descripción	Estos requisitos son considerados como funcionales pues para definir la arquitectura se parte de la necesidad de ajustarse al entorno normativo (de facto o de iure)				
Razón fundamental	La arquitectura debe permitir su implementación en infraestructuras críticas que dependen de un organismo centralizado que exige la adopción de criterios comunes.				

7.1.4. Motivaciones específicas.

Id. Requisito		Tipo de Requisito		Id. Caso de uso	
Descripción	Fortalecimiento de infraestructuras criticas				
Razón fundamental	La importancia en las infraestructuras críticas, dotadas se ha puesto de manifiesto en un conflicto a nivel internacional a escasos miles de km de nuestras fronteras, Ucrania. Resulta significativo que los principales ataques en el ciberespacio a infraestructuras criticas han sido y son a Ucrania y ponen de relevancia la necesidad de establecer, al menos, unas bases de las que partan todos los profesionales y aúnen esfuerzos para la defensa propia y de países con intereses comunes y/o compartidos				
Criterio de valoración	Numero de noticias diarias sobre la guerra híbrida en relación al conflicto con Ucrania				
Documentación	Periódicos nacionales e internacionales				

7.2. Modelado Conceptual

Groso modo, lo que se va a realizar es un modelado conforme a la arquitectura recomendada de un sistema de recepción de paquetería procedente de un avión aterrizado en el aeropuerto de Valencia.

Se trata de una sistema de control industrial que mueve los equipajes de un sitio a otro integrado en una infraestructura critica como es un aeropuerto y que podemos desglosar su modelado mas básico de la siguiente manera:

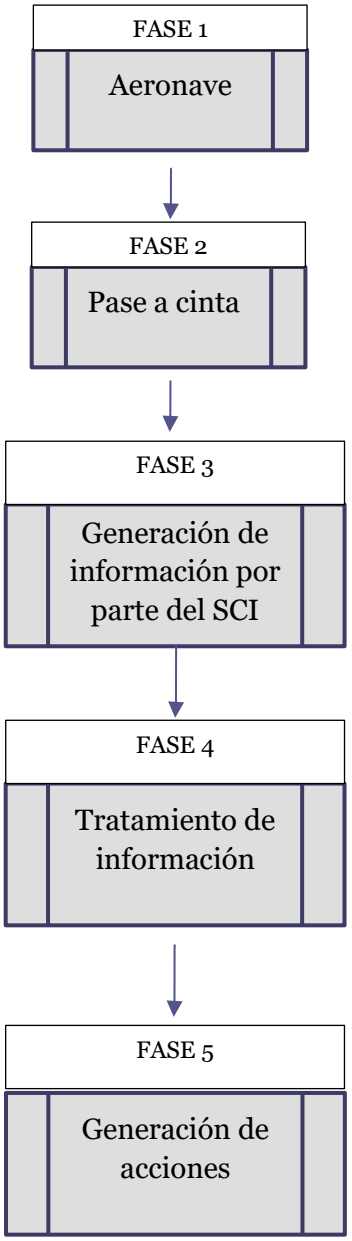
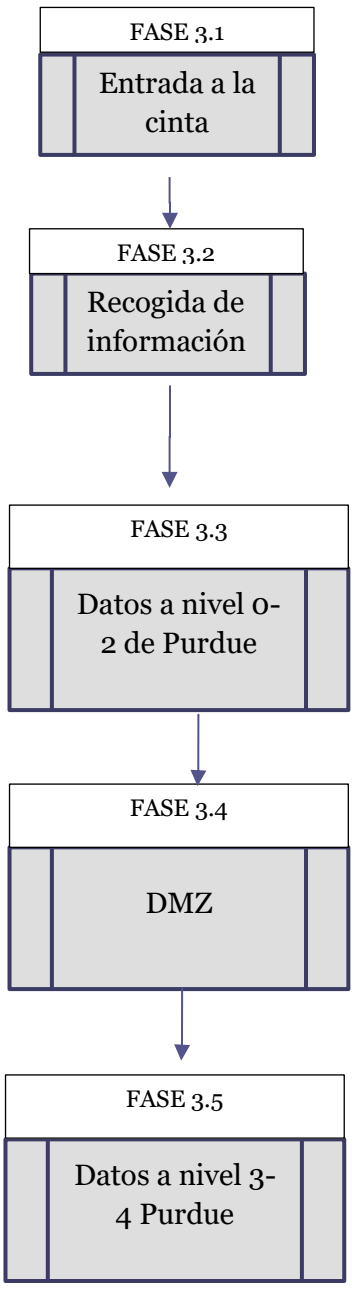
	FASE 1	La carga llega al aeropuerto en la aeronave
	FASE 2	La carga se traslada de la bodega del avión al hangar correspondiente donde hay una cinta que moverá la carga y la clasificará con un sistema de control industrial
	FASE 3	Los sistemas sensores generan información relativa a la carga (peso, color, volumen, código de barras, procedencia, etc.)
	FASE 4	El sistema de control industrial y toda la arquitectura analiza la información y da traslado de las acciones oportunas. En el caso de la cinta le indicará como proceder con la carga
	FASE 5	La carga es clasificada y derivada a una de las opciones del SCI. Asimismo los sistemas de información del aeropuerto reciben los datos de la carga para su correcta gestión (seguimiento, seguridad, desvío, etc.)

Tabla 2 Modelado conceptual general

La parte más importante en lo que a arquitectura de sistema de control industrial en una infraestructura critica que es un aeropuerto es la adquisición de datos de la cinta de equipajes, trasladarlos a los sistemas necesarios, someterlos al tratamiento necesario y generar las acciones oportunas. Asimismo podemos suponer que existe un sistema más global para optimización de procesos (IIoT) relacionado con el concepto de Industria 4.0, pero aplicado a este caso de uso

Se pueden desglosar en:

<table>
<tr><td colspan="3">FASE 3 Generación de información por parte del SCI</td></tr>
<tr><td rowspan="5"> 
</td><td>FASE 3.1</td><td>La carga es depositada en la cinta</td></tr>
<tr><td>FASE 3.2</td><td>Los sistemas sensores recogen la información necesaria, que suponemos es:
Peso
Temperatura
Volumen
Lectura código de barras con información del bulto (origen, destino, trayecto, etapas, identificación material potencialmente peligroso, etc.)</td></tr>
<tr><td>FASE 3.3</td><td>Tratamiento a nivel 0 – 2 de Purdue. Datos de sensores, controladores, HMI de bajo nivel, etc.</td></tr>
<tr><td>FASE 3.4</td><td>Tratamiento DMZ</td></tr>
<tr><td>FASE 3.5</td><td>Tratamiento a nivel 3-4 de Purdue. Niveles operativo para el SCI, logístico y de control del aeropuerto, historiadores, etc.</td></tr>
</table>

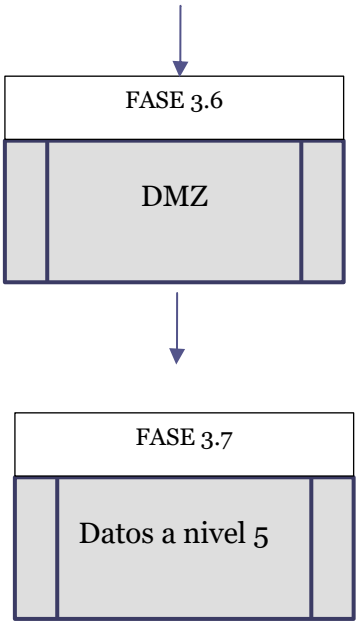
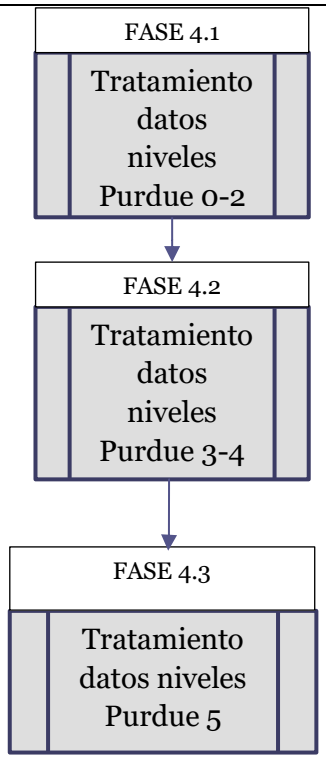
	FASE 3.6	Tratamiento DMZ
	FASE 3.7	Tratamiento a nivel 5 de Purdue. Niveles de empresa y acceso desde el exterior a la información para servicios adicionales (pasajero, empresas de logística, etc.)

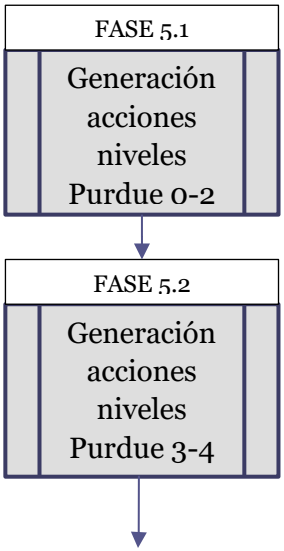
Tabla 3.- Modelado conceptual Generación de información

Y lo mismo ocurrirá con el tratamiento y las acciones derivadas. Se va a obviar una definición de todas las opciones que se pueden adoptar a nivel de negocio en una terminal aeroportuaria, logística, de gestión de procesos, de control industrial, etc. Las actuales tendencias conllevan unas posibilidades, podría decirse, ilimitadas. Sirva de ejemplo, (aunque no lo tomemos para el modelado pero si para ejemplificar hasta donde podría llegarse para empezar) el modelo de arquitectura definido para una arquitectura cognitiva heterogénea para IIoT (Cognitive Heterogeneous Architecture for Industrial IoT) y que integra todos los conceptos más avanzados como son:

- Seguridad basada en PKI acoplada a las claves pre programadas a IoT asociada a un sistema de blockchain.
- Una maquina cognitiva basada en blockchain que identifica cada equipo, clave y cambio de forma univoca para evitar modificaciones maliciosas sobre cualquier elemento.
- Arquitectura en la nube, pero con el matiz de descentralización apoyada en el *edge-computing* que la convierte en *fog-based*.
- Aseguramiento de la seguridad e integridad en y de la operación con una herramienta o maquina de supervisión de la Seguridad orientado a los sistemas mas críticos.
- Un sistema y método cognitivo que, junto con modelos de supervisión, análisis y previsión de nueva generación, permite alcanzar altos niveles de seguridad e integridad.

Dependiendo de los niveles se ha de tomar unas u otras acciones con exigencias varias:

FASE 4 Tratamiento de la información		
	FASE 4.1	Los datos de sistema procedentes de sensores que pueden ser securizados (o no), almacenados temporalmente, enviados, codificados, etc. y luego tratados según los sistemas de planta.
	FASE 4.2	Los datos deben ser almacenados, tratados y enviados, o no a los niveles superiores dependiendo de su interés y con las medidas adecuadas de seguridad. La DMZ se da por contemplada.
	FASE 4.3	Tratamiento de dato a nivel empresa o de cara a usuarios externos. Uso de DMZ necesario.

FASE 5. Generación de acciones		
	FASE 5.1	Los sistemas de célula/línea reciben las ordenes necesarias de los elementos de control para continuar con su funcionamiento conforme al sistema
	FASE 5.2	Las acciones que implican los terminales de operador, historiador, etc. se generan a esta nivel y condicionan tanto a niveles inferiores como superiores

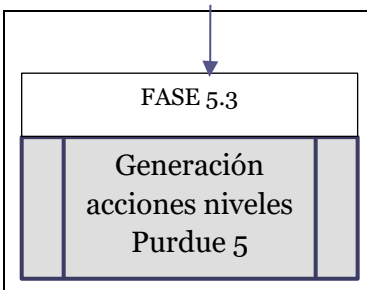
	FASE 5.3	A nivel de empresa se llevan a cabo unas acciones que repercuten más en el negocio, o en la operatividad de la organización o de la instalación total.

Tabla 4.- Modelado conceptual Generación de Acciones

7.3. Análisis de la seguridad

La seguridad es la razón de ser de la arquitectura motivo de este Trabajo. El análisis de la seguridad se saca de cada uno de los puntos del estado del arte y de la solución propuesta.

Básicamente, la seguridad se basa en:

- separar los elementos por niveles
- dar seguridad a cada uno de dichos elementos
- poner elementos entre niveles para monitorizar y detectar problemas de seguridad
- asegurar las comunicaciones (entre elementos, de los operadores, del exterior de la organización, intra-organización, etc.)

No obstante, la seguridad se garantiza siguiendo las guías de las entidades de acreditación que tienen autoridad sobre la organización que gobierna la instalación o infraestructura crítica.

Los modelos planteados son los que, a priori, ofrecen las mejores garantías, aunque dependerán siempre de los sistemas que finalmente se elijan y se instalen en dicha arquitectura y en el correcto desempeño de la organización para implementar el ciclo de seguridad completo.

7.4. Análisis del marco legal y ético

El marco legal para la definición de un SCI es uno, pero para infraestructuras críticas es mucho más exigente y detallado.

Lo primero es identificar una infraestructura critica, que se lleva a cabo en la Directiva europea 2008/114/CE del 8 de diciembre de 2008 (CCN-CERT). Pero esto solo es el principio. Después, se podrían enumerar un elevado número de normativas, más o menos generalistas dependiendo del sistema de control industrial, de la infraestructura crítica que sea, de los datos que se traten, del tipo de empresa que gestiona esa infraestructura, etc.

Así por ejemplo en nuestro caso de uso, los datos de un equipaje y de su responsable podrían ser datos de carácter personal y estarían sometidos a la Ley Orgánica de protección de Datos y Garantía de derechos Digitales….

Un buen resumen de normativa aplicable se establece en la guía de INCIBE *"Cumplimiento legal"* (CUMPLIMIENTO LEGAL), de donde se extrae la siguiente figura:

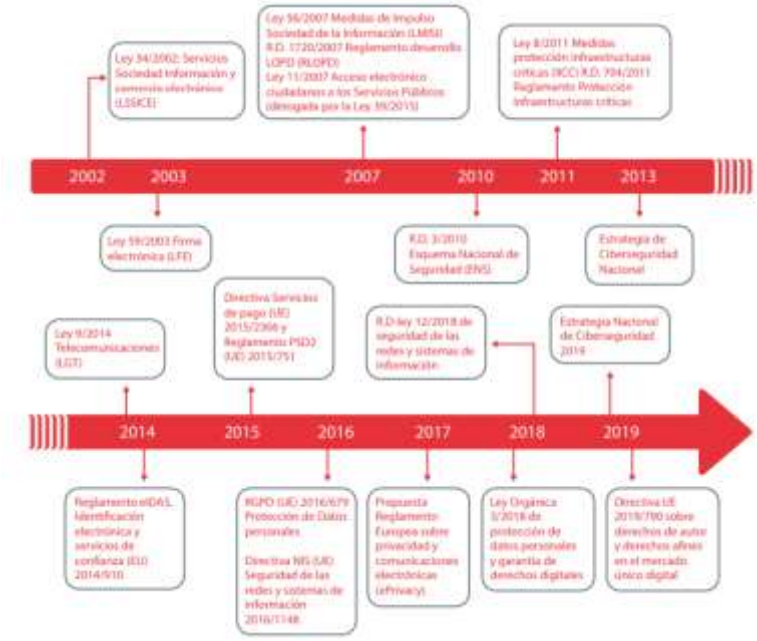


Figura 36 .- Desarrollo legal en materia de Ciberseguridad

Esta figura resume en cierta medida el ímprobo marco normativo aplicable, pero sirva la misma únicamente para remitir al organismo regulador que mantiene actualizada una base de conocimiento de referencia para este tipo de sistemas y a la que hay que ajustarse para garantizar el máximo nivel de cumplimiento legal.

7.5. Propiedad intelectual

Todo el SW sugerido en este trabajo es *Open Source*, y todo el material utilizado procede de fabricación propia a partir de la experiencia y formación recibidas o bien de documentos de instituciones públicas cuya misión es generar contenido para su uso, como es INCIBE.

7.6. Identificación y análisis de soluciones posibles

La solución al problema de garantizar la seguridad en una arquitectura de SCI para infraestructuras críticas no es única. Se podría decir que hay tantas como agentes libre pensantes interesados en la seguridad.

No obstante, y tal y como se menciona mas arriba, se ha planteado una solución basada en la arquitectura actual de INCIBE para infraestructuras críticas, apoyándonos en criterios del primer planteamiento de arquitectura, el modelo Purdue. El objetivo es buscar un conglomerado de conceptos más antiguos y más actuales que generen esa arquitectura aplicable a toda infraestructura y que sea susceptibles de obtener los sellos de garantía de seguridad por la entidad competente en el ámbito nacional.

8. Solución propuesta

Para dar solución al problema se plantearán varias arquitecturas y los elementos necesarios para implementarlas y probar su funcionamiento, todo con SW o simuladores opensource

8.1. Plan de Trabajo

Se ha partido de una herramienta de gestión de proyectos open *source* como es Project Libre que ofrece unas capacidades limitadas pero suficientes para plantear el trabajo e ir tratando las desviaciones.

Un desglose básico de la planificación llevada a efecto, con los ajustes derivados del devenir del desarrollo del TFM sería el capturado en distintas imágenes mas abajo. Las fechas han ido cambiando como en cualquier proyecto conforme se han dado los acontecimientos (vacaciones, imponderables académicos/profesionales/personales, etc.) aunque se muestra un resumen bastante ajustado del tiempo dedicado a cada tarea:

	Nombre	Duracion	Inicio	Terminado	Predecesores
1	Conseguir tutor	17 days?	1/10/21 8:00	25/10/21 17:00	
2	Proponer tema y gestionar autorizaciones	17 days?	1/10/21 8:00	25/10/21 17:00	
3	Establecer el alcance	10 days?	25/10/21 8:00	5/11/21 17:00	2
4	Establecer estructura acorde a formato, propuesta y alcance	5 days?	8/11/21 8:00	12/11/21 17:00	3
5	Estado del arte I Bases	76 days?	15/11/21 8:00	28/02/22 17:00	4
6	Estado del arte II IoT	76 days?	15/11/21 8:00	28/02/22 17:00	4
7	Estado del Arte III INCIBE	76 days?	15/11/21 8:00	28/02/22 17:00	4
8	Analsis del problema	54 days?	1/03/22 8:00	13/05/22 17:00	5
9	Definición de requisitos	13,875 days?	1/03/22 8:00	18/03/22 16:00	5
10	Modelo conceptual	36,125 days?	18/03/22 16:00	9/05/22 17:00	9
11	Otras consideraciones del análisis conformea plantilla	4 days?	9/05/22 8:00	12/05/22 17:00	10
12	Solucion propuesta	30 days?	13/05/22 8:00	23/06/22 17:00	11
13	Ajustes y revisiones	5 days?	27/06/22 7:00	1/07/22 17:00	12
14	Utlimas aportaciones, turnitin y ebron	5 days?	4/07/22 8:00	8/07/22 17:00	13

Tabla 5.- Diagrama de Gantt

Este software es bastante limitado y ofrece pocas opciones para exportar imágenes o informes que se puedan trasladar o ajustar a cualquier formato de archivo. A continuación se muestra una imagen general del proyecto y la inicial y final que muestre el nombre de la tarea y las fechas mas signficativas

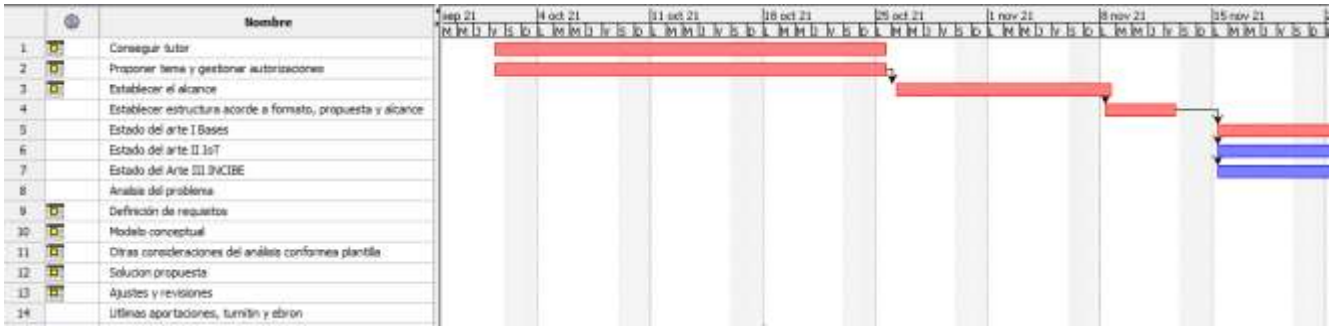


Tabla 6.- Diagrama de Gantt II

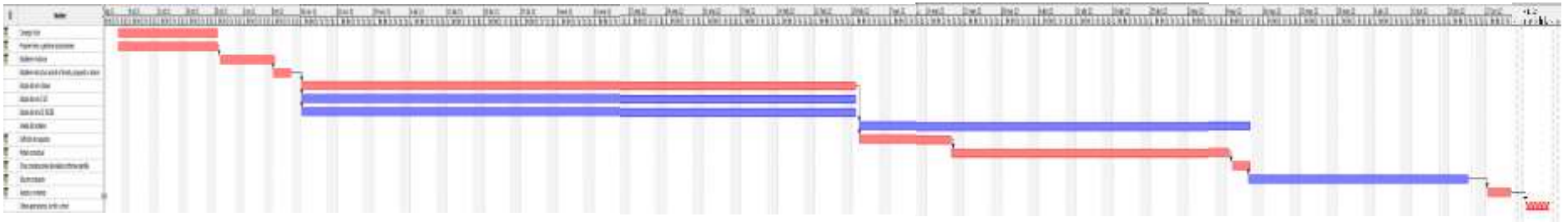


Tabla 7 .- Diagrama de Gantt III

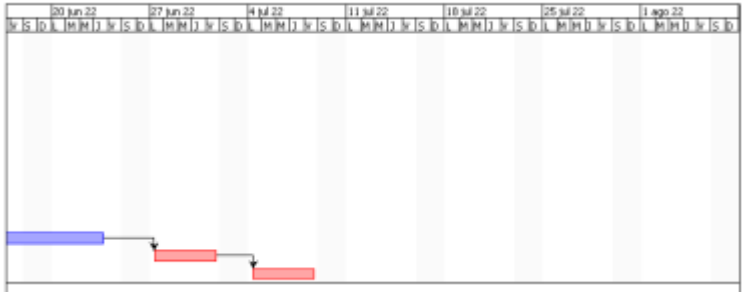


Tabla 8 .- Diagrama de Gantt IV

8.2. Diseño de la solución

La solución que se propone para una arquitectura segura de SCI con IoT/IIoT para infraestructuras críticas parte de los conceptos vistos y de las recomendaciones de INCIBE-CERT.

Consta de una arquitectura general, con los conceptos específicos a considerar y una arquitectura detallada con un ejemplo donde se especifican los elementos posibles, identificando uno de manera concreta y los requisitos de dichos elementos y la interconexión entre ellos.

8.3. Arquitectura General del Sistema

8.3.1. Planteamiento

El planteamiento esta orientado a la norma IEC 62443-4-2 que es la seguida por INCIBE, organismo nacional que puede certificar y que dispone de guías y fórmulas de consulta fiables (INCIBE-CERT, 2022). En dicha norma se describen los requisitos para alcanzar un nivel de seguridad por un SCI. Además, los fabricantes se pueden ajustar a esta norma para permitir su integración directa de subsistemas en sistemas mayores. Son susceptibles, por lo tanto, de seguir esta arquitectura tanto los propietarios de activos, como proveedores de producto, integradores de sistema y autoridades de cumplimiento.

8.3.1. Componentes

Se definen en un SCI cuatro tipos de componentes, que son:

- Aplicaciones software – AS -, tales como antivirus o software SCADA.
- Dispositivos embebidos – DE—que podrían ser IED (*Intelligent Electronic Devices*), PLC, etc.
- Dispositivos host – DH -, especialmente importantes son las estaciones de ingeniería, el historiador de datos y la maquina de control de operaciones.
- Dispositivos de red –DR --, como *firewalls*, *switches* y *routers*.

Para cada uno de los elementos se matizan los requisitos y los niveles de seguridad definidos. Se parte de una situación supuestamente madura en seguridad dentro de la organización, que haya seguido o este progresando en la integración de sus procesos en marcos de referencia de seguridad (NIST CyberSecurity Framework 1.1, 2018). Así por ejemplo, si la organización esta implantando un sistema de gestión de la seguridad en un sistema, se habrá asegurado de:

- Disponer de:
  - Segmentación en las redes existentes,
  - Operaciones procedimientadas,

- un inventario de activos TO adecuado (datos, aplicaciones, hardware industrial, red, tecnología, personal, instalaciones, etc.) con la información adecuada (nombre, descripción, etc. incluyendo una valoración según el impacto en el negocio o misión de la organización según se vean afectados parámetros como disponibilidad, integridad, confidencialidad, confidencialidad, criticidad y coste)

Figura 37 .- Ejemplo de clasificación de activos (INCIBE-CERT)

- ciberseguridad en la cultura de los empleados (formación / concienciación).

- Realizar un análisis de riesgos que ayude a dar la criticidad de cada sistema de la empresa en su totalidad.

- A continuación, por cada sistema, se determinarán las zonas y conductos y un nivel de seguridad objetivo (SL-T, *Target Security Level*) para cada uno. Las zonas de seguridad se definen en el estándar como "agrupaciones de activos físicos o lógicos que comparten requisitos comunes de seguridad, las cuales tienen la frontera (física o lógica) claramente definida". Las conexiones entre estas zonas se denominan conductos y deben incluir medidas de seguridad para controlar el acceso a las mismas, resistir ataques de denegación de servicio, evitar la propagación de cualquier otro tipo de ataque, hacer de escudo para otros sistemas de la red y proteger la integridad y la confidencialidad de las comunicaciones.

- Asimismo, se valorará la seguridad alcanzada (SL-A, *Achieved Security Level*), dando una idea del nivel de seguridad que se presenta.

- Si los niveles de seguridad disponibles no son los deseados hay que calcular el nivel que se podría alcanzar cambiando la configuración, esto es calcular nivel de seguridad según capacidad (SL-C, *Capability* Security Level).

- En este punto se comprobará si, se puede lograr el SL-T fijado o si hace falta tomar medidas adicionales compensatorias, como la adquisición de nuevos equipos o la modificación de la arquitectura de red.

8.3.2. Una primera aproximación

De cara a la protección de la terminal de equipajes que queremos simular en el aeropuerto, se genera una primera aproximación a una arquitectura SCI tipo que es la sugerida por INCIBE.

En nuestro caso podemos aproximar la terminal de manera que:

- Zona 0 – zona de tratamiento de equipajes donde lo deposita el personal de línea dedicado a carga y descarga. Consta de diferentes zonas, aunque en este trabajo consideraremos solo la zona F1 donde habrá una cinta clasificadora de equipaje que deriva los bultos a diferentes sitios y que puede tener otro tipo de equipamiento. En esta zona estaría el equipamiento SCADA.
- Zona D – zona para elementos del sistema de control que se escalarán a la red de negocio, como pueden ser historiadores
- Zona C – zona para la red de la terminal dedicada al control de paquetes, difusión de información al resto de terminales (pantallas información, enlaces, etc.)
- Zona B – una DMZ para acceso dar protección especial de cara a Internet y permitir accesos remotos externos, acceso online a información de todo el aeropuerto (p.ej. cinta de equipajes para vuelo procedente de X con hora de llegada prevista YY en terminal ZZ)

En cada una de estas zonas hay que incorporar los elementos de seguridad que mas adelante se detallan para permitir la monitorización, control, respuesta etc. ante los eventos de seguridad que se den.

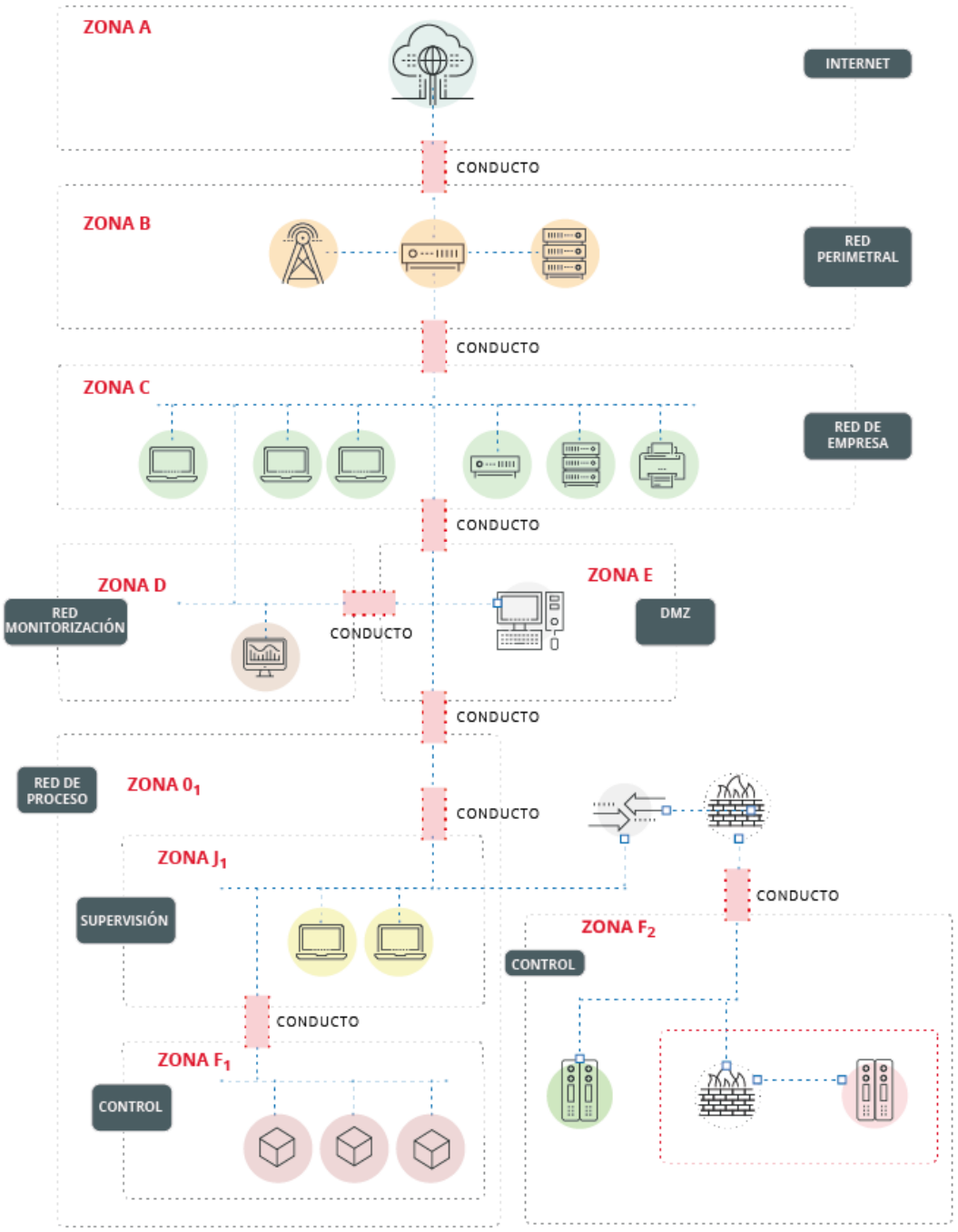


Figura 38 .- Primera aproximación a una solución de arquitectura

En cada nivel se establecen los niveles de seguridad de seguridad (SIL Safety *Integrity Levels*) que se han descrito mas arriba, y se añaden los niveles de seguridad mencionados en el punto anterior:

- SL-T (Niveles de Seguridad Objetivo), que según la norma será 2,3 y 4 para los procesos críticos, aunque la criticidad la determina la organización entre las posibles:
    - Nivel de seguridad 0: no requiere especificaciones o protecciones de seguridad.

- Nivel de seguridad 1: requiere de protección contra incidentes no intencionados.
- Nivel de seguridad 2: requiere de protección contra incidentes intencionados, perpetrados con medios sencillos, pocos recursos, conocimientos básicos y baja motivación.
- Nivel de seguridad 3: requiere de protección contra incidentes intencionados, perpetrados con medios avanzados, recursos suficientes, conocimientos medios y motivación media.
- Nivel de seguridad 4: requiere de protección contra incidentes intencionados, perpetrados con medios muy avanzados, grandes recursos, conocimientos avanzados y motivación alta.

- SL-C (Niveles de seguridad según capacidad) y
- SL-A (Niveles de seguridad alcanzados).

Si una zona o conducto tiene un SL-C es que todo lo que hay dentro esta capacitado para desarrollar las funciones de seguridad de ese nivel. Esas funciones se definen para cada nivel e identifican por lo tanto las capacidades de un dispositivo, zona, conducto, etc. Las capacidades de seguridad se clasifican en 7 requisitos fundamentales: Confidencialidad de los Datos (CD), Restricción del Flujo de Datos (RFD), Tiempo de Respuesta ante Eventos (TRE), Identificación y Control de Autentificación (ICA), Control de Uso (CU), Integridad de Sistema (IS) , y Disponibilidad de Recursos (DR).

Cada requisito contiene distintas capacidades de seguridad estructurada en niveles, pudiendo un dispositivo certificado en nivel de seguridad 1 SL-1 cumplir todos los requisitos con las capacidades hasta ese nivel, aunque puede ser mas interesante saber con que nivel se cumple determinado requisito. Así por ejemplo con una tabla como la de la siguiente ilustración se identifica cómo adquirir más nivel de seguridad en el requisito ICA a partir de sus requisitos de sistema (o componente, según lo que estemos valorando) y de mejora:

Requisitos	SL1	SL2	SL3	SL4
RF 1 - Identificación y control de autentificación				
RS 1.1 – Identificación y control de usuarios	✓	✓	✓	✓
RM (1) Identificación única		✓	✓	✓
RM (2) Autentificación de múltiples factores en redes no probadas			✓	✓
RM (3) Autentificación de múltiples factores en todas las redes				✓

Figura 39 .- Ejemplo requisitos de sistema y de mejora para un nivel de seguridad en un requisito fundamental

Con estos requerimientos y requisitos fundamentales, se definen los niveles de seguridad mediante un vector: SL- X ([FR], Dominio)= {ICA, CU, IS, CD, RFD, TRE, DR}, siendo X, el que estemos evaluando: A, C o T.

8.3.3. Elementos de seguridad ciber

Dado que es un trabajo que gira en torno a la seguridad cabe señalar los principales elementos que van a permitir la monitorización de la red y que permitirán segmentarla y establecer criterios de seguridad y que son IDS, IPS y SIEM o recolector de eventos:

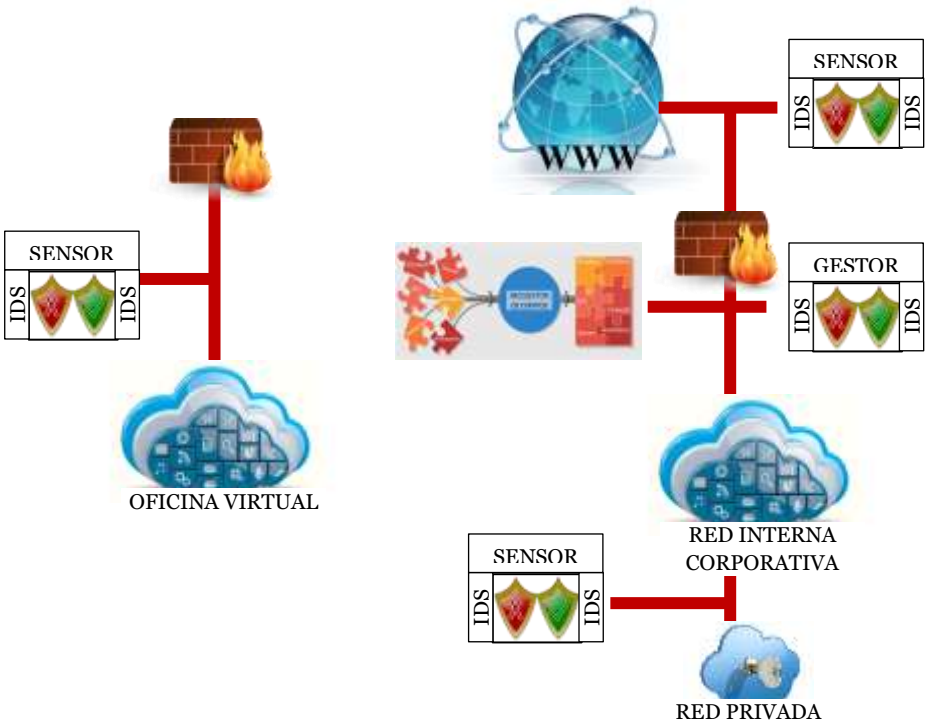


Figura 40 .- Elementos básicos ciber para una red SCI segura

8.4. Diseño Detallado

La red que se va a implementar a modo de laboratorio en la medida de elementos disponibles *OpenSource* que ofrezcan ciertas garantías sería la propuesta por INCIBE en (INCIBE) y que se muestra en la siguiente ilustración

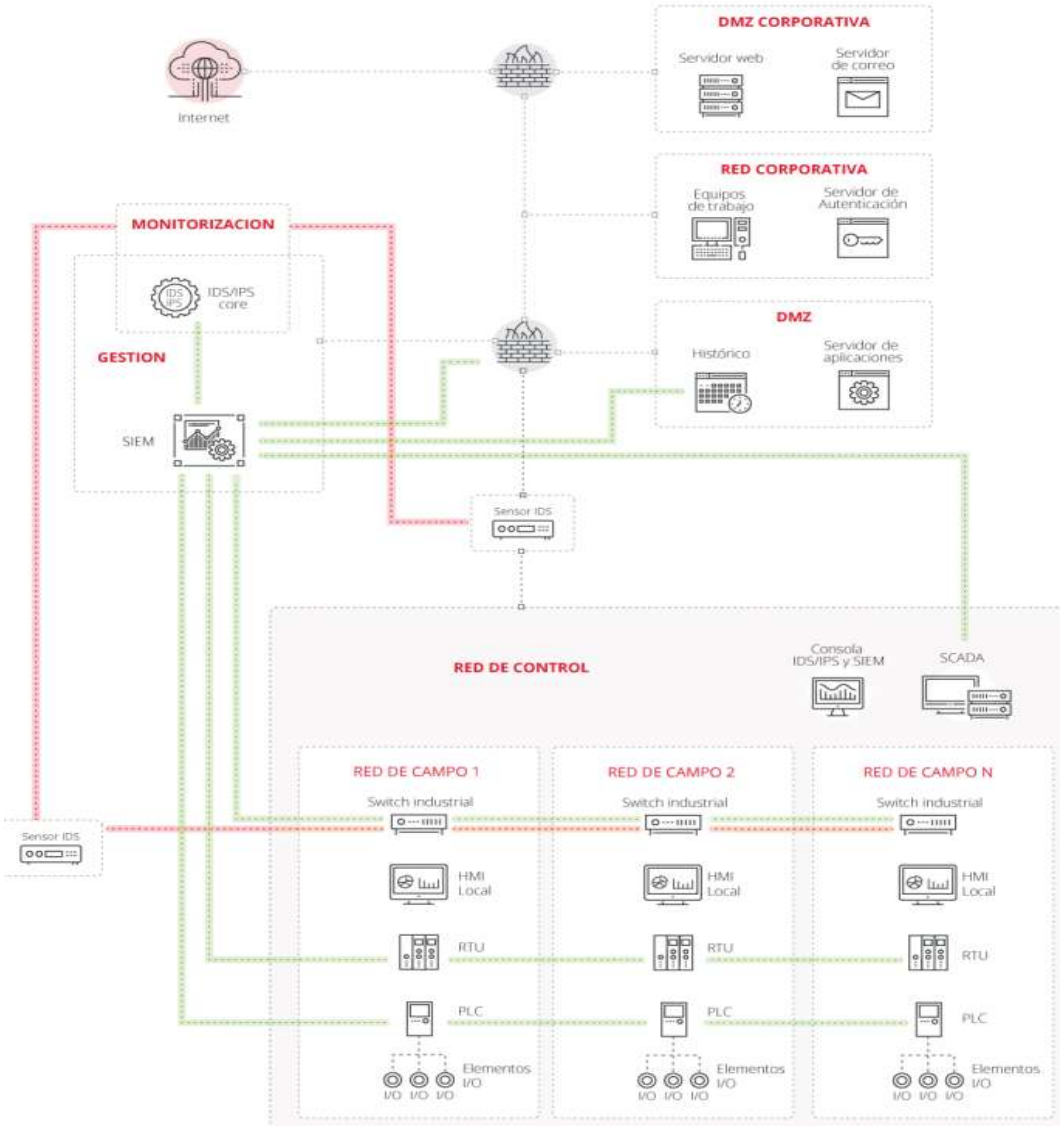


Figura 41 .- Arquitectura Unificada SIEM, IDS e IPS

Esta red se ajusta a los niveles Purdue y a los especificados en la norma IEC 62443 y que de forma general vemos en la siguiente figura:

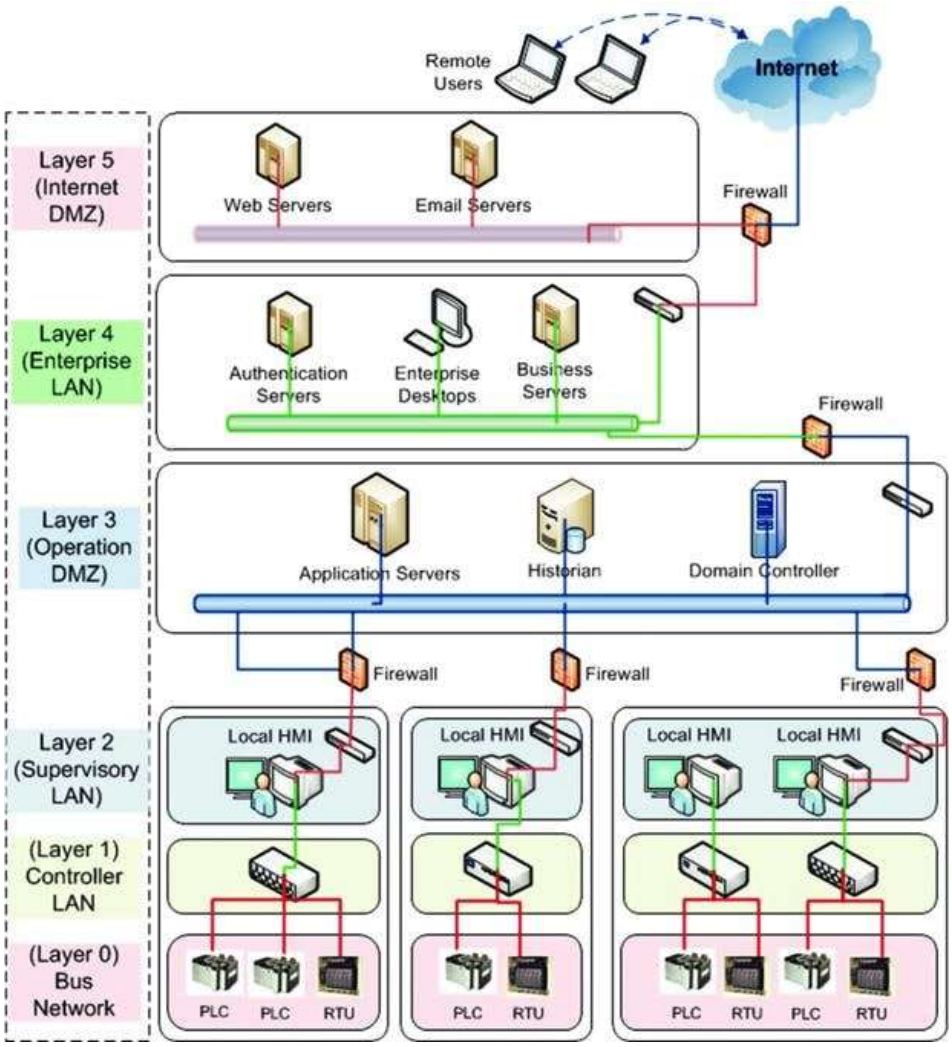


Figura 42 .- Arquitectura IEC 62443 (Onward Security)

Aunque se distinguen 5 niveles, para la propuesta se consideran tres:

- Un nivel de sistemas de control para los sistemas SCADA y los sistemas de control industrial en si.(Zona 0)
- Un nivel de empresa para los sistemas generales, donde se puede separa la parte de negocio relacionada con el SCI (operaciones) y el resto de la actividad de la empresa. (Zonas C y D)
- Un nivel exterior a la empresa, desde el que se ofrecen servicios de todos los niveles: negocio, operaciones y control

Entre los distintos niveles se instalan elementos de seguridad y se implementan zonas desmilitarizadas para ofrecer información y servicios de manera segura, tanto en un sentido como en otro.

La arquitectura dispone, además, de:

IDS – con las reglas para alertar de cara a la interpretación por consola del operario o administrador de seguridad. Gestionarían el tráfico entre campo y control. Podrá bloquear el trafico que de lugar a un fallo de seguridad, por lo

que la monitorización se hará haciendo pasar dicho trafico por el sensor IDS y no mediante puertos espejo.

IPS – se aconseja su uso en los niveles superiores para el intercambio de información entre control y parte corporativa/negocio

SIEM – deberá estar en los sistemas de control para poder acceder a los eventos de logs de **todos** los dispositivos, lo cual puede suponer una carga que exija una red paralela para esta función que no menoscabe la operatividad de la red de control. Incluirá, por lo tanto los logs de dispositivos de campo, de red e igualmente los de IDS e IPS.

8.5. Tecnología Utilizada

En aras de hacer un planteamiento más completo se supone que se parte de una red inicial similar a la siguiente

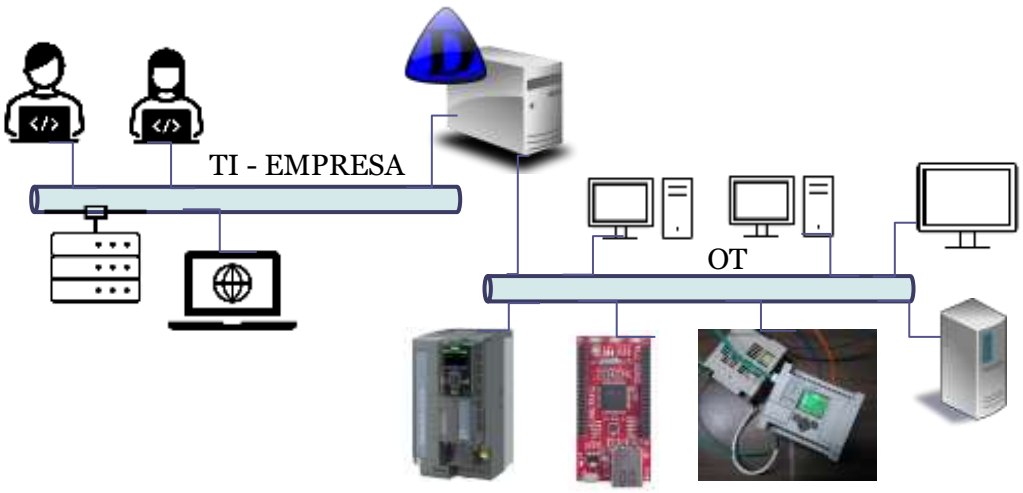


Figura 43 .- Configuración inicial red

En esta red se dispondrá de dos segmentos de red principales: uno de IT para los servicios de la empresa; y otro OT para el área industrial de que dispone dicha empresa. El elemento que las interconecta o que comparten es el servidor de dominio.

Esta configuración es manifiestamente insegura y no cuenta con los niveles de los que se ha venido hablando durante este trabajo. Hay que segmentar la red e incorporar elementos de seguridad y separación entre redes que permitan monitorizar el tráfico y prevenir y detectar incidentes.

Se pretenden implementar algo similar a las figuras anteriores:

- Una red OT separada de la TI mediante un firewall. Se genera un área de industria (*zone* o *cell*), una zona de supervisión y control con SCADA, HMI, etc. y una DMZ para operaciones y lo que haya que "exportar" a la red TI (historiadores, logs, etc.). Se incorporaría una plataforma

multifunción tipo *Arduino*/*RaspberryPi* para introducir características IIoT

- Una red TI separada del exterior con un firewall y una DMZ para dar servicios a ese "exterior". Habría un área de servicios generales que en principio debería estar separada de la OT como DNS y similar.
- Una interconexión con el exterior.
- Un sistema de detección y prevención de incidentes con información de toda índole.

Seria una configuración básica sin:

- Capa de empresa y capa de negocio separadas
- Un par de firewalls para separar la zona de TI y la OT, aunque lo recomendado es evitar esa *three-legs firewall configuration*.
- Una estructura de seguridad paralela para TI, dado que el trabajo gira en torno a OT

Con las herramientas que se enumeran a continuación se implementaría la siguiente arquitectura:

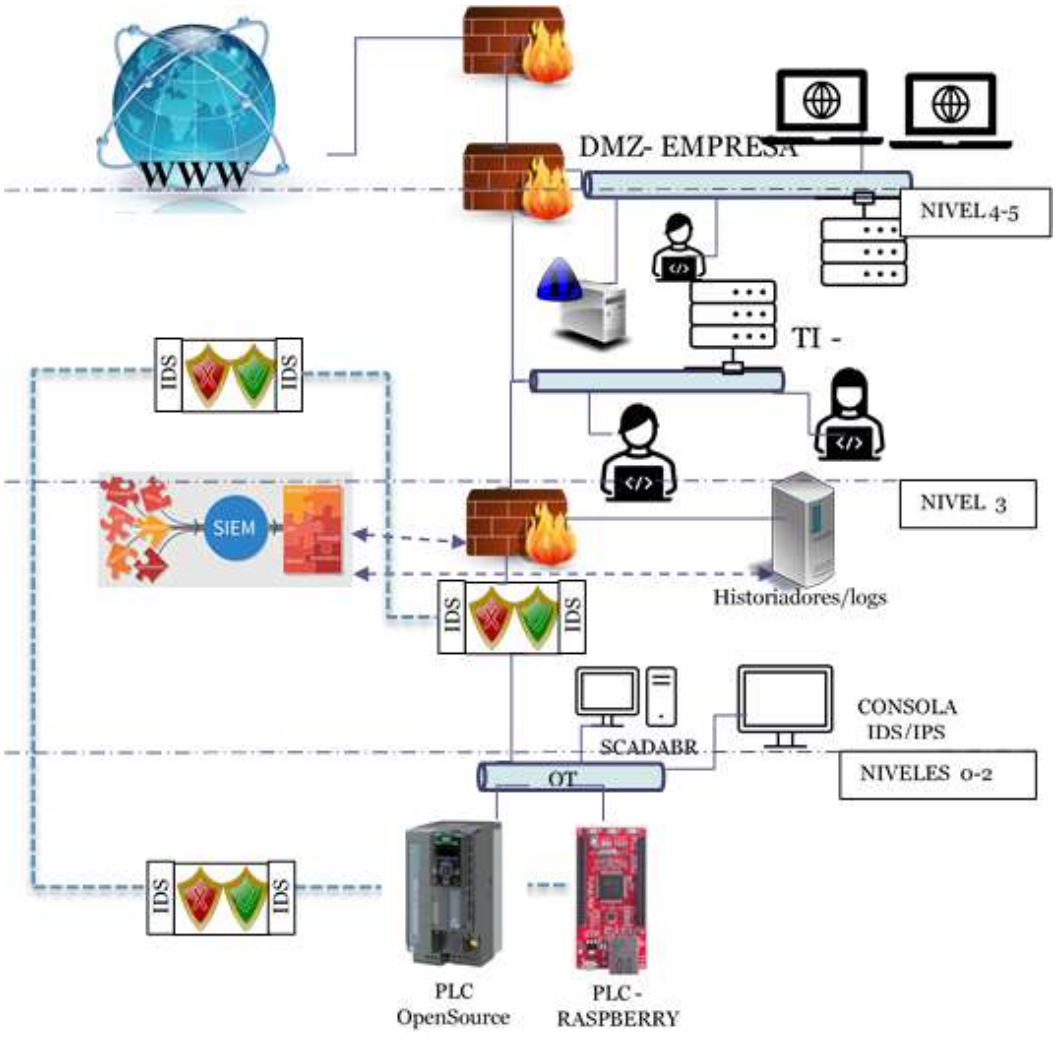


Figura 44 .- Arquitectura objetivo

8.6. Desarrollo de la solución propuesta

La solución propuesta consta del siguiente SW:

Nivel Purdue	SW	Descripción
0-2	*OpenPLC*	Software de simulación de *PLCs*
	Factory IO	Software de modelización de procesos industriales en 3D. Version Trial 30 días
3	*Raspberry* PI	Simulación plataforma opensource
3	SCADABR	SCADA opensource
4-5	Windows Server 2019	S.O Versión 30 días
4-5	Windows 10	S. O Versión 30 días
	SNORT/SNORTBY	IPS/IDS opensource

Tabla 9 .- Configuración de escenario I

La idea es simular una proceso industrial con FactoryIO, controlado por PLCs simulados con *OpenPLC*, montado también sobre un *Raspberry* Pi que representa el mundo IoT, integrados en un SCADA simulado con SCADA-BR que corre sobre maquinas Windows que pueden ser Server o Workstations. Este ultimo SW se usaría para montar maquinas virtuales que muevan el software de control industrial.

Por la parte de seguridad se propone el SW que aparece en las guías de INCIBE, que es SNORT con sus complementos adecuados para poder monitorizar y exportar alarmas.

8.6.1. Proceso de instalación y configuración

La configuración del SW sobre las distintas maquinas del escenario sería la siguiente:

- *OpenPLC* – Software de simulación de *PLCs*

SECUENCIA DE PASOS	COMANDO
Obtener el proyecto de Github	git clone https://github.com/thiagoralves/OpenPLC_v3.git
Entrar a la carpeta de proyecto	cd OpenPLC_v3
Ejecutar el instalador para Linux	./install.sh Linux

Abrir la dirección sobre el 8080:	El login por defecto es: *openplc* / openplc
Instalar drivers sobre *OpenPLC* que habilitarán el uso de entradas y salidas físicas, como si de un PLC estándar se tratara.	Hardware → seleccionar el driver más adecuado para nuestro entorno

Tabla 10 .- Configuración de escenario II

- FactoryIO – Software simulador y modelización de procesos, con trial de 30 días.

  Se elegirá uno de los escenarios básicos que da la plataforma por simplicidad. Se configura el de clasificación mediante un sensor de color del objeto, que es el más aproximado al que leería el código de barras de un paquete o equipaje para su tratamiento de la terminal de carga.

  Se dispone de una cinta transportadora de entrada donde se deposita el equipaje, un lector del color del bulto y una cinta de salida con tres rampas de selección según el color sea rojo, verde u otro. En el caso del presente documento sería dotar al sistema con un lector de código de barras y/o el identificador de color de que ya dispone y a la cinta de salida con tantas rampas como clasificaciones tuviésemos del equipaje: origen, destino, trayecto, etapas, identificación material potencialmente peligroso, etc.

Figura 45 .- Cinta de clasificación de paquetería y equipajes I

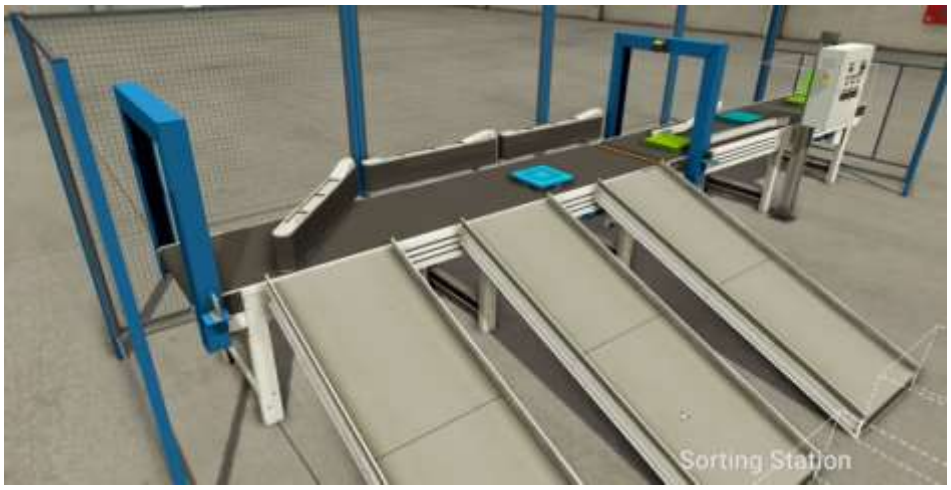


Figura 46 .- Cinta de clasificación de paquetería y equipajes II

La instalación se lleva a efecto sobre una maquina Windows y la configuración supone la interconexión de cada interfaz del SCI con los PLCs del sistema

- SCADABR – SCADA opensource de capacidades limitadas que permite la implementación del sistema y monitorización de trafico entre elementos.

SECUENCIA DE PASOS	COMANDO
Obtener el proyecto de Github	git clone https://github.com/thiagoralves/SCADABR_Installer.git
Entrar a la carpeta de proyecto	cd SCADABR_Installer
Ejecutar el instalador para Linux	./install.sh Linux

Tabla 11 .- Configuración de escenario III

- SNORT –IPS opensource para el escenario. Se realiza su instalación sobre un Ubuntu Server 16.04

SECUENCIA DE PASOS	COMANDO
Instalar librerías necesarias previas a la instalación	apt install libdnet libdnet-dev libpcap-dev make automake gc flex bison libdumbnetdev
Crear enlaces simbólicos por cambio de nombre	ln –s /usr/include/dumbnet.h /usr/include/dnet.h ldconfig
Instalar paquete de Linux, que será en /etc./snort	Apt install snort
Instalar el complemento Data AcQuisition Library (DAQ) para modo INLINE	wget https://www.snort.org/downloads/snort/daq-X.X.X.tar.gz tar zxf daq-X.X.X.tar.gz cd daq-X.X.X ./configure make && make install ldconfig
Ejecutar el instalador para Linux	./install.sh Linux
Configurar modo INLINE en el fichero *snort.conf*	ipvar HOME_NET 192.168.1.0/24 #Modificar al rango de red concreto ipvar EXTERNAL_NET !HOME_NET config daq: afpacket config daq_mode: inline
Añadir reglas de bloqueo y demás correspondientes a sistemas industriales	(Digital Bond's IDS/IPS rules for ICS and ICS protocols., 2022)

(proyecto Quickdraw de DigitalBond)	
Configurar modo INLINE según distribución LINUX en fichero snort.debian.conf	DEBIAN_SNORT_INTERFACES = “eth0:eth1” #poner las dos interfaces sobre las que va a estar inspeccionando el tráfico Snort

Tabla 12 .- Configuración de escenario IV

- Barnyard. Complemento de *Snort* para el envío de alertas que se generan en local al sistema de gestión de eventos (SIEM) que se tenga

SECUENCIA DE PASOS	COMANDO
Descargar Banyard2 y dependencias	apt install libtool git clone https://github.com/firnsy/barnyard2.git
Instalar y configurara	./autogen.sh ./configure make && make install
Configurar sistema destinatario de alarmas SIEM en fichero banyard.conf: base de datos, usuario/contraseña, IP host BD, etc.	output database alert,mysql user=usuario password=contraseña dbname=nombre_bbdd host=host_remoto
Configurar formato salida del fichero de salida en snort.conf	output unified2: filename fichero limit 128
Iniciar banyard2	barnyard2 –c /etc/snort/barnyard2.conf –d /var/log/snort –f snort.conf –w /var/log/snort/barnyard2.waldo

Tabla 13 .- Configuración de escenario V

- *Snorby*... Sistema de gestión de eventos opensource (SIEM) orientado al manejo e interpretación de los datos generados con *Snort*.

SECUENCIA DE PASOS	COMANDO
Instalar paquetes accesorios: base de datos para almacenar la información (*mysql*) y apache para su despliegue por ser aplicación web	apt install apache2 apach2-dev mysql-server libmysqlclient-dev ruby-full postgreesql-server-dev-9.5 libcurl4-apoenssl-dev
Creación base de datos con su usuario/contrase-a	mysql -u root -p > create database snorby; > create user 'usuario@'%' identified by 'contraseña' > grant all privileges on snorby.* to usuario@'%' with grant option; > flush privileges; > quit
Descarga Snortby en carpeta apache	git clone https://github.com/Snorby/snorby.git cp –r snorby /var/www/html
Configuración/modificación ficheros Gemfile por version de SW	GEMFILE gem 'rake', '0.9.2' ➓ gem 'rake', '> 0.9.2' despues de gem 'json','X.X' añadir ➓ gem 'thin' en el apartado group (:development) to comentar ➓ gem 'thin' GEMFILE.LOCK gem 'rake', '0.9.2' ➓ gem 'rake', '> 0.9.2'
Instalar gemas de ruby y crear ficheros de configuración	gem install rails bundler passenger wkhtmltopdf do_postgres –v '0.10.16' bundle install cp config/snorby_config.yml.example config/snorby_config.yml cp config/database.yml.example config/database.yml
Configurar acceso a base de datos en database.yml	Base de datos Usuario/contraseña
Instalar SW de integración Snorby- ruby_Apache	passenger-install-apache2-module

Crear y añadir a snorby.conf líneas generadas en la instalación	touch /etc/apache2/sites-available/snorby.conf LoadModule passenger_module /var/lib/gems/2.3.0/gems/passenger-5.0.30/buildout/apache2/mod_passenger.so PassengerRoot /var/lib/gems/2.3.0/gems/passenger-5.0.30 PassengerDefaultRuby /usr/bin/ruby2.3
Configurar/modificar snorby.confs	Servername 192.168.1.200 DocumentRoot /var/www/html/snorby/public <Directory /var/www/html/> AllowOverride all Order allow,deny Allow from all Options –MultiViews </Directory>
Configurar lectura desde Snorby con enlace	ln -s /etc/apache2/sites-available/snorby.conf /etc/apache2/sites-enabled/snorby.conf rm /etc/apache2/sites-enabled/000-default.conf
Iniciar Snorby para mostrar alertas de Snort	RAILS_ENV=production bundle exec rake snorby:setup
Acceder a través del navegador	Usuario snortby@example.com Password: snorby

Tabla 14 .- Configuración de escenario VI

9. Resultados

Los resultados obtenidos son:

1. Un análisis de las tecnologías para sistemas de control industrial en infraestructuras críticas incorporando IoT
2. Un análisis de las arquitecturas propuestas por entidades nacionales, supranacionales, de ámbito gubernamental y, por último, entidades asociadas a entidades asociación de empresas

3. Una infraestructura que es considerada segura por la autoridad certificadora nacional.

4. Un caso de uso donde aplicar los resultados obtenidos: una infraestructura crítica con un sistema de control industrial integrado en un todo multipropósito. Esto es, una cinta de equipajes, el sistema de selección de bultos, una terminal de carga y un aeropuerto como podría ser el de Valencia

5. Un listado de software opensource o con periodos de prueba para poder simular el caso de uso

Los resultados que se esperaban obtener se extendían a la simulación de la infraestructura, pero los recursos requeridos para ello no han podido conseguirse. En los distintos intentos realizados se ha podido comprobar que simular la arquitectura objetivo de la Figura 45, habría hecho falta:

- Entorno industrial
    - 1 maquina Linux para PLC
    - 1 maquina virtual simulando una *raspberry*-pi que representase el mundo IoT
    - 1 maquina virtual para el SCADA
    - 1 maquina virtual para el historiador
    - 1 maquina virtual para una Workstation (aunque simular además un HMI seria ideal)
- Entorno IT
    - 1 maquina virtual para un controlador de dominio (aunque lo recomendable es que hubiese dos)
    - 2 maquina virtual para simular una red IT de negocio/empresa intentando simular un nivel 4 y un nivel 5 de PURDUE
- Infraestructura de seguridad
    - 3 maquina virtual para un IDS/IPS a nivel de red de dispositivo, de control y concentrador para reenvío a SIEM
    - 1 maquina virtual para un SIEM
    - 3 maquinas virtuales para firewalls básicos

Esto nos permitiría ver que el trafico esta filtrado, analizado y tratado en cada transición en los niveles adecuados, que es saliendo de la celda/planta industrial y, grosso modo, se contemplaría la complejidad y la seguridad obtenida.

No obstante se ofrece como resultado el software y los comandos necesarios para la configuración de aquellos más específicos del mundo de SCI y de la arquitectura de seguridad.

10. Conclusiones

Parece demostrada mediante las diferentes referencias la importancia que tienen los SCI y las infraestructuras críticas para el desarrollo de la sociedad como la conocemos. De esa importancia dimana el interés en su protección.

Asimismo se han desarrollado tendencias como IIoT que permiten aumentar la eficiencia mediante la monitorización, obtención de información, tratamiento de la misma y corrección de desviaciones en un proceso industrial en tiempo real. Esta tendencia, junto con otras tecnologías, genera la Industria 4.0 que mejoran la productividad de cualquier sistema y la eficiencia en el funcionamiento de una infraestructura basada en SCI.

Esas mejoras conllevan un riesgo si no se llevan a cabo de manera segura, un riesgo que se manifiesta para la operación de la infraestructura, para la seguridad del sistema y para los datos asociados a sistemas jerárquicamente superiores con los que se relacione y que hace que se propague, en un caso extremo, el riesgo de una central de análisis de aguas a las decisiones de alto nivel relativas a la seguridad nacional.

Una infraestructura crítica se compone de diferentes sistemas de control industrial cuyo primer reto es poner seguridad a todos sus dispositivos, a los accesos locales y remotos a los mismos, por multitud de personas que acceden con diferentes privilegios en distintos momentos de la vida del sistema (que es mucho mas largo de partida que un sistema IT). El primer movimiento clave en cualquier organización es identificar los riesgos y securizar sus infraestructuras para minimizarlos. Ello conlleva la planificación de soluciones que se puedan implementar eficientemente. La mejor manera de afrontar este reto es por niveles, es decir, fijar una arquitectura por niveles ajustable a cualquier sistema con una serie de soluciones base aceptadas por la comunidad tecnológica e industrial y que no solo sean aplicables sino reconocibles, auditables y acreditables conforme a entidades comunes con la autoridad suficiente para avalar cánones de máxima seguridad.

Antes de entrar en niveles de sistemas de control industrial y sistemas asociados cabe señalar cuatro niveles para contemplar la seguridad que hay que garantizar:

- Seguridad física, con infraestructuras de acceso restringido, cuyas zonas estén compartimentadas y con control de personal que manipula los equipos y sistemas o simplemente transita por las instalaciones. Los procedimientos de acceso y trabajo a las instalaciones y equipos deben estar en constante revisión y puestos a prueba para su correcta ejecución y poder así garantizar tanto el entrenamiento del personal como la eficacia de las medidas tomadas.
- Seguridad de red o en las comunicaciones, con equipos cada vez más conectados, más inteligentes y más capaces de dar interfaces locales y remotos. Esto hace que lo mas recomendable sea separar por áreas y niveles los sistemas de manera que la información sea controlada cuando sale o entra y el control de la infraestructura solo se puede hacer tras pasar los elementos de seguridad que se instalan y que van mas allá de un firewall que separe la red de control de la red de la empresa.
- Seguridad del sistema y de su integridad, con un concepto de seguridad a nivel de sistema mas allá de aquel que garantice su operación de manera segura para el técnico, el sistema y el entorno de cara a la producción o eficiencia, sino que garantice la seguridad ciber en todo los niveles: en el diseño de sistemas con la seguridad como requisito, en la fabricación de sus elementos, en su distribución, en su instalación y puesta en marcha, etc.
- Seguridad en la organización, con la seguridad establecida culturalmente entre el personal, en la visión y misión de la empresa, en sus distintas

políticas y objetivos, visto como un proceso de mejora continua, etc. Dentro de esa seguridad en la empresa como un pilar, la idea de tener centralizado la monitorización, detección y respuesta ante incidentes es más que deseable, aunque con una estructura por niveles que refuerce sus capacidades y que minimice el efecto de una brecha de seguridad en algún elemento, sistema o nivel.

El primer objetivo, que rezaba *"Establecer una arquitectura segura para sistemas de control industrial que integren IoT."* se ha alcanzado mediante estos niveles en los que después se entra para definir qué funciones implementar y con qué elementos.

Viendo todo esto, se ha verificado que en cualquier SCI y en cualquier infraestructura crítica se puede y se debe establecer seguridad

- Tecnológica por niveles de manera relativamente fácil y no demasiado costosa, aunque, como no podía ser de otra manera, la inversión en esta área repercutirá de manera directa en la seguridad total.
- Conceptual en la empresa con no poco esfuerzo, pero con un retorno mucho mas rápido y rico que lo que a priori pudiera parecer. Esto supone una incorporación del concepto de seguridad en cada área de la empresa, en cada empleado, en cada proceso, etc. tal y como se ha expresado más arriba.

Los dos siguientes objetivos, que eran:

- *Definir unas condiciones de contexto tecnológicas, normativas, políticas, etc. que integren al máximo las exigencias necesarias para lo que se considera seguridad.*
- *Establecer los elementos necesarios en la tecnología, en los procesos, en las políticas, etc. para una arquitectura segura.*

Se pueden considerar cubiertos tanto en los distintos puntos del estado del arte como en el planteamiento del problema, donde se definen arquitecturas tipo, políticas y guías, y se establece una relación entre el elemento teórico y su implementación práctica.

No obstante, como conclusión practica a todo lo anterior mas evidente y orientado al ultimo objetivo (*Plantear un caso de uso*) hemos visto como un SCI de una terminal aérea se puede reproducir si se dispone de los medios adecuados con opensource y adaptándose a un esquema de difusión nacional y avalado por un entidad acreditadora que garantiza cada paso y elemento de dicha arquitectura. No obstante, se han propuesto soluciones intermedias, aunque igualmente se han identificado soluciones ideales que maximicen la seguridad, como por ejemplo:

- DMZ separadas entre niveles para el trafico de entrada y salida
- DMZ para historiadores y sistemas de nivel 3-4
- Firewalls en entrada a cada nivel separados para cada frontera (en lugar de un solo firewall de tres interfaces para nivel superior, inferior y dmz). Esto es, en una frontera entre niveles, un firewall gobernado por el equipo de seguridad del nivel superior que controla lo que entra y sale de su nivel y otro en el nivel inferior.
- Etc.

Como líneas de trabajo futuras se podría apuntar a aquello que no se ha podido realizar en su totalidad como es la implementación virtualizada de todo lo recogido en el TFM. Las pruebas que se han hecho exigían unos recursos que no soportaban el despliegue de todas las maquinas (sistemas simulados de planta tanto PLC como IoT, sistema SCADA, historiadores, sistemas IT, sistemas de *routing*, elementos y sistemas de seguridad, etc.). La implementación presenta un horizonte lleno de pruebas y demostraciones capaces de desarrollar entornos donde simular herramientas aplicables al ámbito industrial (optimización de procesos, ejercicios *digital twin*, etc.), herramientas de seguridad (*pentesting*, laboratorio formación, etc.) y de IT (integración IT/OT, etc.).

11. Referencias

AENA. (s.f.). Obtenido de www.aena.es: https://www.aena.es/es/negocioscomerciales/negocios-comerciales/carga/carga-valencia/centro-carga-aerea.html

Black hills. (2019). Obtenido de Information Security: https://www.blackhillsinfosec.com/tag/anti-virus/

CCN-CERT. (s.f.). Obtenido de DIRECTIVA 2008/114/CE DEL CONSEJO DE LA UNIÓN EUROPEA: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Cibersecurity & Infrastucture Security Agency. (05 de 2022).

CISA. (16 de 05 de 2022). Obtenido de https://www.cisa.gov/critical-infrastructure-and-key-resources-support-annex

Cognitive Heterogeneous Architecture for Industrial IoT. (s.f.). Obtenido de https://ec.europa.eu/info/index_en: https://cordis.europa.eu/project/id/780075

Conficker Worm – A Worm That Affects Microsoft Windows. (03 de 2022). Obtenido de studycorgi.com: https://studycorgi.com/conficker-worm-a-worm-that-affects-microsoft-windows/

crossco.com. (s.f.). Obtenido de crossco.com: https://www.crossco.com/resources/articles/determining-safety-integrity-levels-for-your-process-application/

CUMPLIMIENTO LEGAL. (s.f.). Obtenido de INCIBE: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf

Cyber Security 4.0: Protecting the Industrial Internet of Things. (s.f.). Obtenido de https://www.c4iiot.eu/: https://www.c4iiot.eu/wp-content/uploads/2020/08/c4iiot-r1.3.pdf

Cybercity. (2009). Obtenido de Selinux vx apparmor: https://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html

Cybersecurity & Infrastucture Security Agency. (2017). Obtenido de ICS Advisory (ICSA-17-264-04): https://www.cisa.gov/uscert/ics/advisories/ICSA-17-264-04

Cyybersecirity & Infrastructure Security Agency. (16 de 05 de 2022). Obtenido de https://www.cisa.gov/ics

DesignNews –. (s.f.). Obtenido de “Integrated Safety Breaks the Cost-Savings Barrier at Plants” : https://goo.gl/fro2KS

Digital Bond's IDS/IPS rules for ICS and ICS protocols. (25 de 06 de 2022). Obtenido de Github: https://github.com/digitalbond/Quickdraw-Snort

European Union Agency for Cybersecurity. (2022). Obtenido de https://www.enisa.europa.eu/

exida.com. (s.f.). Obtenido de https://www.exida.com/Alarm-Management

Fireeye.com. (Dic de 2017). Obtenido de https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

ics-cert.kaspersky.com. (17 de 03 de 2021). Obtenido de https://ics-cert.kaspersky.com/media/Kaspersky-ICS-engineering-and-integration-sector-2020-En.pdf

IEC 62351. (s.f.). Obtenido de Wikipedia: https://en.wikipedia.org/wiki/IEC_62351

IEC WebStore International Electrotechnical commisssion. (s.f.). Obtenido de IEC 62443-4-1:2018 : https://webstore.iec.ch/publication/33615

IETF.ORG. (s.f.). Obtenido de https://www.ietf.org/rfc/rfc2119.txt

INCIBE. (s.f.). Obtenido de Configuración IDS,IPS y SIEM: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf

INCIBE-CERT. (s.f.). Obtenido de Inventario de Activos y gestión de la seguridad en SCI: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

INCIBE-CERT. (2022). Obtenido de blog: https://www.incibe-cert.es/blog/el-iec-62443-4-2-necesidad-securizar-los-componentes

Industry IoT Consortium. (2019). Obtenido de https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

Internationl Society of Automation. (2022). Obtenido de ISA/IEC 62443 Cybersecurity Series Designated as IEC Horizontal Standards: https://www.isa.org/intech-home/2021/december-2021/departments/isa-iec-62443-cybersecurity-series-designated-as-i

Interrnet of Things Architecture. (2022). Obtenido de https://www.iot-a.eu/#:~:text=IoT-A%2C%20the%20European%20Lighthouse%20Integrated%20Project%20addressing%20the,foundations%20for%20fostering%20a%20future%20Internet%20of%20Things.

ISO/IEC 27001 Information Security Management. (s.f.). Obtenido de https://www.iso.org/isoiec-27001-information-security.html

ISO-IEC International Organization for Standarization. (s.f.). Obtenido de Internet of Things (IoT) - Reference Architecture: https://www.iso.org/standard/65695.html

Lynis, an introduction. (s.f.). Obtenido de CISOFY Auditing hardening compliance: https://cisofy.com/lynis/

Ministerio de transporte, movilidad y agenda urbana. (s.f.). Obtenido de https://www.mitma.gob.es/: https://www.mitma.gob.es/recursos_mfom/01_lenguaje_transporte_intermodal.pdf

National Computer Security Incident. (05 de 2022). Obtenido de Response Teams (CSIRTs) Response Teams (CSIRTs): https://www.sei.cmu.edu/our-work/cybersecurity-center-development/national-csirts/index.cfm

National Council of ISACs. (s.f.). Obtenido de https://www.nationalisacs.org/

National Vulnerability Database USA. (s.f.). Obtenido de http://nvd.nist.gov/home.cfm

NIST - Computer Security Resource Center. (s.f.). Obtenido de Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

NIST CyberSecurity Framework 1.1. (2018). Obtenido de https://www.nist.gov/cyberframework

NIST Cybersecurity Framework. (05 de 2022). Obtenido de https://www.nist.gov/cyberframework

North American electric Reliability Corporation. (s.f.). Obtenido de https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

OSISoft, is not part of AVEVA. (s.f.). Obtenido de https://www.osisoft.com/pi-system/#tab1

OWASP.ORG. (16 de 05 de 2022). Obtenido de https://owasp.org/www-project-top-ten/

RTOS. (s.f.). Obtenido de WWW.DIGIKEY.ES: https://www.digikey.es/es/articles/real-time-operating-systems-and-their-applications

Siemens. (s.f.). Obtenido de SINAMICS Overview: https://goo.gl/TbrEk9

Software Engineering Institute and Carnegie Mellon for US-CERT. (s.f.). Obtenido de http://www.cert.org/other_sources/viruses.html

Stuxnet 0.5: The Missing Link. (2013). Obtenido de https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

United Nations. (s.f.). Obtenido de Objetivos y metas de desarrollo sostenible: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

US-CERT vulnerability Notes Database. (s.f.). Obtenido de http://www.kb.cert.org/vuls/

Volere. (s.f.). Obtenido de https://www.volere.org/templates/volere-requirements-specification-template/

Wikimedia.ORG. (s.f.). Obtenido de https://upload.wikimedia.org/wikipedia/commons/7/77/Unix_history-simple.svg

WIKIPEDIA. (s.f.). Obtenido de Gestión de información y eventos de seguridad: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad

Wikipedia. (2022). Obtenido de Wiipedia: https://en.wikipedia.org/wiki/List_of_automation_protocols

Wikipedia. (16 de 05 de 2022). Obtenido de Operational Historian: https://en.wikipedia.org/wiki/Operational_historian

www.microsoft.com. (2022). Obtenido de docs.microsoft.com: https://docs.microsoft.com/es-es/azure/architecture/reference-architectures/iot

12. Glosario

- IDS (*Intrusion Detection System*)….Sistema de detección de intrusos es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia. Utilizan un diccionario de firmas de tráfico y en caso de actividad sospechosa emiten una alerta.

- IPS (*Intrusion Prevention System*)….Software que se utiliza para proteger a los sistemas de ataques y e intrusiones. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos. Llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, además de lanzar alarmas, descartar paquetes o conexiones. Pueden encontrarse sistemas que unen capacidades y que se denominan UTM (Unified *Threat Management*)

- SIEM (*Security Information and Event Manager*).... sistema de gestión de eventos e información de seguridad: es una solución híbrida centralizada que engloba dentro de la seguridad del sistema la gestión de información (*Security Information Management*) y la de eventos (*Security Event Manager*). La tecnología SIEM proporciona un análisis en tiempo real de y sobre las alertas de hw y sw de la red. Recoge los registros de actividad (*logs*) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas. (WIKIPEDIA)

- NGF (*Next Generation Firewall*).... Un firewall de próxima generación (NGFW) es un dispositivo de seguridad de red que proporciona capacidades avanzadas como el conocimiento y control de aplicaciones, la prevención de intrusiones integrada y la inteligencia de amenazas entregada en la nube., etc.

13. Anexo.- Objetivos de Desarrollo Sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**			X	
ODS 2. **Hambre cero.**			X	
ODS 3. **Salud y bienestar.**				X
ODS 4. **Educación de calidad.**				X
ODS 5. **Igualdad de género.**			X	
ODS 6. **Agua limpia y saneamiento.**	X			
ODS 7. **Energía asequible y no contaminante.**		X		
ODS 8. **Trabajo decente y crecimiento económico.**		X		
ODS 9. **Industria, innovación e infraestructuras.**		X		
ODS 10. **Reducción de las desigualdades**.			X	
ODS 11. **Ciudades y comunidades sostenibles**.		X		
ODS 12. **Producción y consumo responsables.**		X		
ODS 13. **Acción por el clima.**			X	
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**	X			
ODS 17. **Alianzas para lograr objetivos.**	X			

El presente trabajo da una arquitectura segura para sistemas de control industrial en infraestructuras críticas. Su implantación tiene un impacto directo en muchos de los objetivos de desarrollo sostenible. El objetivo es la seguridad, pero su consecución resulta en una arquitectura con los medios adecuados, y un uso en la medida adecuada.

ODS 1 y 2.- La seguridad es uno de los principios de la buena convivencia y la igualdad entre todos los que comparten un espacio común. El planeta Tierra es ese espacio común donde deberíamos vivir de manera segura y a partir de lo cual las desigualdades se minimizarían. Desigualdades a nivel económico y pobreza, entre otras, que se ven plasmada de manera fundamental en la falta de atención a necesidades básicas como son la alimentación. Un mundo seguro facilitaría un reparto mejor de riqueza o al menos una diferencia menor entre los más ricos y los más pobres, desapareciendo la pobreza y el hambre en su concepción actual.

ODS 5 y 10.- De manera análoga a lo anterior, un mundo seguro garantiza la igualdad entre los diferentes colectivos que se puedan establecer por razón de origen, religión o género. Este último criterio, que tanta brecha genera, se vería minimizado en un entorno seguro y libre.

ODS 6.- Teniendo en cuenta que las plantas de tratamiento de aguas son considerados normalmente infraestructuras críticas y están totalmente supeditadas a la correcta operación de sistemas de control industrial, el impacto es altísimo.

ODS 7, 8 y 9.- Una arquitectura segura garantiza una gestión adecuada de los recursos que se tengan que si se ven optimizados procuran un uso eficaz y eficiente de la energía de los sistemas y de las personas. Esto repercute en unan industria capaz de generar empleo digno, con crecimiento económico si otros factores lo permiten y en equilibrio con el medio natural donde se desenvuelve la actividad, minimizando contaminación e impacto medioambiental.

ODS 11 y 12.- En línea con lo anterior, unas infraestructuras seguras, bien compartimentadas y optimizadas dan lugar a una sociedad con servicios sostenibles y producidos de manera responsable.

ODS 16 y 17.- Estos dos objetivos son los que sin lugar a duda presentan mayor grado de relación. Un lugar seguro, es el entorno básico para obtener la paz, justicia e instituciones sólidas que consigan conciliar los intereses de todos. Y esto es mucho mas fácil de conseguir si se hace de manera global (en todos los ámbitos local, regional, nacional, supranacional y mundial) por todos los agentes que participen. El hecho de referirse este trabajo a las autoridades y entidades autorizadas en el ámbito nacional.

ETS Enginyeria Informàtica
Camí de Vera, s/n. 46022. València
T +34 963 877 210
F +34 963 877 219
etsinf@upvnet.upv.es - www.inf.upv.es